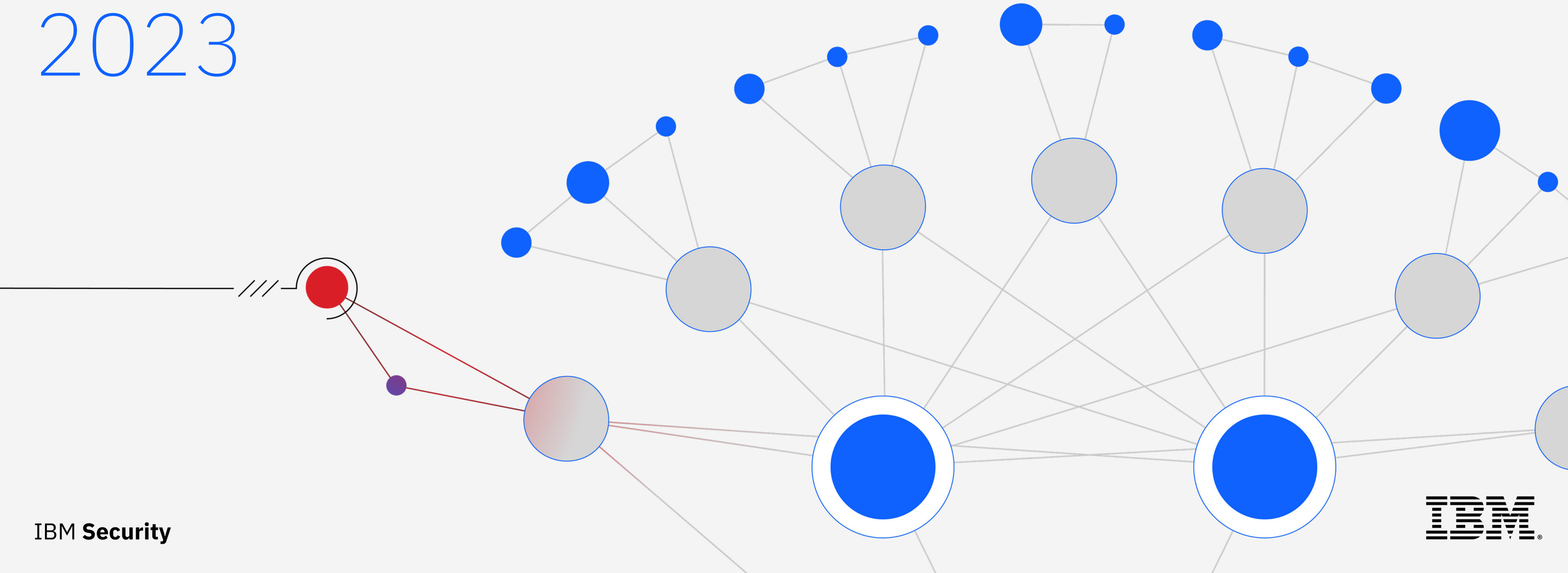
X-Force Threat Intelligence Index 2023

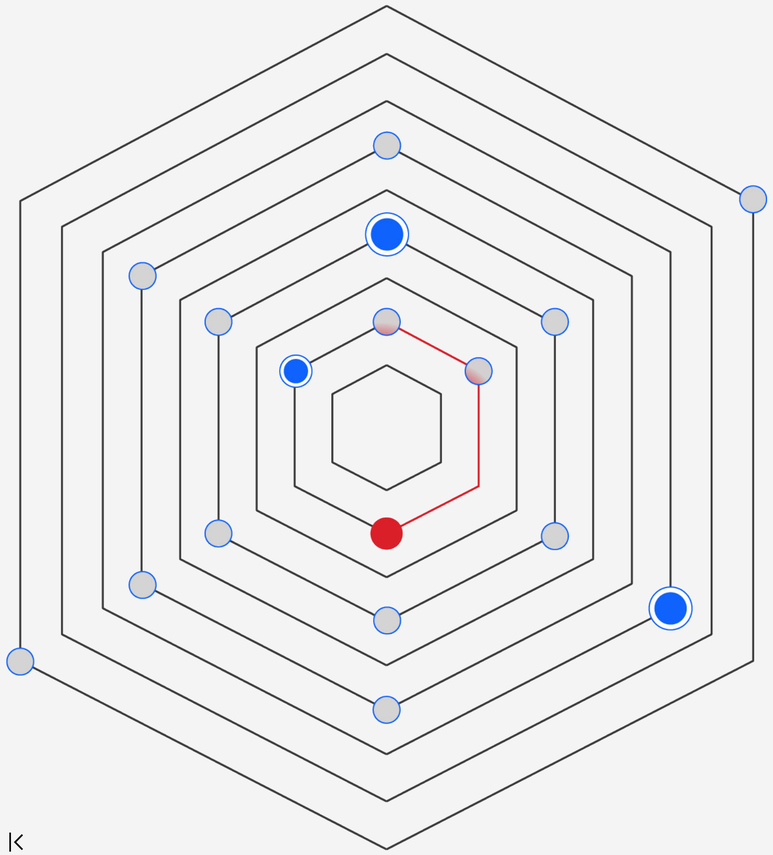


IBM **Security**

Inhaltsverzeichnis

01

Zusammenfassung



2022 war ein weiteres turbulentes Jahr für die Cybersicherheit. Es gab in dieser Hinsicht viele Ereignisse, aber zu den wichtigsten zählten die anhaltenden Auswirkungen der Pandemie und der Ausbruch des militärischen Konflikts in der Ukraine. Umbrüche haben 2022 zu sowohl wirtschaftlichen und geopolitischen als auch gesellschaftlichen Veränderungen und Kosten geführt – und genau das Chaos geschaffen, in dem Cyberkriminelle erfolgreich agieren können.

Und das haben sie auch getan.

IBM Security® X-Force® hat opportunistische Bedrohungsakteure beobachtet, die sich die chaotische Situation zunutze machen, um Regierungen und Unternehmen auf der ganzen Welt zu infiltrieren.

Der IBM Security X-Force Threat Intelligence Index 2023 verfolgt neue und bestehende Trends sowie Angriffsmuster und umfasst Milliarden von Datenpunkten von Netzwerk- und Endpunktgeräten, Incident Response (IR)-Einsätzen, Schwachstellen- und Exploit-Datenbanken und mehr. Dieser Bericht enthält eine umfassende Aufstellung unserer Forschungsdaten von Januar bis Dezember 2022.

Wir stellen diese Ergebnisse als Ressource für IBM Kunden, Forscher auf dem Gebiet der Cybersicherheit, politische Entscheidungsträger, die Medien und die erweiterte Community der Sicherheitsspezialisten und Branchenführer zur Verfügung. Die heutige instabile Situation mit immer komplexeren und böswilligeren Bedrohungen erfordert gemeinsame Anstrengungen zum Schutz von Unternehmen, Bürgerinnen und Bürgern. Mehr denn je benötigen Sie Bedrohungsdaten und Erkenntnisse über Ihre Sicherheitsumgebung, um Angreifern einen Schritt voraus zu sein und Ihre wichtigsten Ressourcen zu schützen.

Damit auch Sie erfolgreich agieren können.

Wie sich unsere Datenanalyse für 2022 geändert hat

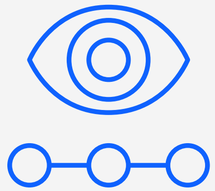
Seit 2022 haben wir die Vorgehensweise, wie wir Teile unserer Daten untersuchen, maßgeblich verändert. Die Änderungen ermöglichen uns aussagekräftigere Analysen und eine stärkere Orientierung an Industriestandards. Dies verhilft Ihnen dazu, fundiertere Sicherheitsentscheidungen zu treffen und Ihr Unternehmen besser vor Bedrohungen zu schützen.

Zu den Änderungen in unserer Analyse im Jahr 2022 gehören:

- **Ursprüngliche Zugriffsvektoren:** Durch die Übernahme des MITRE ATT&CK-Frameworks zur Nachverfolgung ursprünglicher Zugriffsvektoren können wir unsere Forschungsergebnisse besser auf die breitere Cybersicherheitsbranche abstimmen und wichtige Trends auf technischer Ebene erkennen.
- **Exploits und Zero-Day-Schwachstellen:** Durch Extrapolation aus unserer robusten Schwachstellendatenbank, die Daten aus fast 30 Jahren umfasst, können wir unsere Analyse in einen Kontext stellen und die tatsächliche Bedrohung durch Sicherheitslücken ermitteln. Dieser Prozess steht auch im Zusammenhang mit dem schwindenden Anteil an gezielt eingesetzten Exploits und wirkungsvollen Zero Days.
- **Methoden der Bedrohungsakteure und ihre Auswirkungen:** Indem wir die Schritte, die Bedrohungsakteure während eines Angriffs unternehmen, von den tatsächlichen Auswirkungen eines Vorfalls getrennt haben, konnten wir die kritischen Phasen des Vorfalls identifizieren. Dabei wurden wiederum Bereiche erkannt, auf die die Responder nach einem Störfall vorbereitet sein sollten.

02

Wesentliche Erkenntnisse



Die wichtigsten beobachteten Angriffsmethoden: Bei fast einem Viertel aller im Jahr 2022 behobenen Vorfälle war mit 21 % die Bereitstellung von Backdoors die häufigste Methode. Vor allem die zu Beginn des Jahres beobachtete Zunahme von Emotet, einer vielseitig einsetzbaren Malware, trug wesentlich zum Anstieg der Backdoor-Aktivitäten im Vergleich zum Vorjahr bei. Auch wenn die Anzahl der Backdoor-Aktivitäten anstieg, machte Ransomware, die seit mindestens 2020 an erster Stelle steht, mit 17 % einen Großteil der Störfälle aus, was die anhaltende Bedrohung durch diese Malware unterstreicht.

Erpressung war die häufigste Auswirkung von Angriffen auf Unternehmen: Erpressung war mit 27 % eindeutig das beliebteste Mittel der Bedrohungsakteure. 30 % der Vorfälle, die zu Erpressungen führten, betrafen Unternehmen aus der Fertigungsbranche, da Cyberkriminelle weiterhin die angespannte Lage dieser Branche ausnutzten.

Phishing war der wichtigste ursprüngliche Zugriffsvektor: Phishing ist nach wie vor der führende Infektionsvektor, der bei 41 % der Vorfälle ermittelt wurde, gefolgt von der Ausnutzung von Anwendungen mit Internet-Schnittstelle in 26 % der Fälle. Infektionen durch schädliche Makros sind in den Hintergrund getreten, was vermutlich auf die Entscheidung von Microsoft zurückzuführen ist, Makros standardmäßig zu blockieren. Die Verwendung schädlicher ISO- und LNK-Dateien hat sich im Jahr 2022 zur wichtigsten Taktik für die Verbreitung von Malware durch Spam entwickelt.

Zunahme von Hacktivismus und zerstörerischer Malware: Russlands Krieg in der Ukraine öffnete die Tür zu einem von vielen aus der Cybersicherheit-Community erwarteten Demonstrationsbeispiel dafür, wie Cybertechnologie die moderne Kriegsführung ermöglicht. Obwohl sich die schlimmsten Vorhersagen zum Zeitpunkt der Veröffentlichung dieses Berichts nicht bewahrheitet haben, gab es ein bemerkenswertes Wiederaufleben von Hacktivismus und zerstörerischer Malware. X-Force beobachtete auch beispiellose Veränderungen in der Welt der Cyberkriminalität mit einer verstärkten Zusammenarbeit zwischen cyberkriminellen Gruppen und Trickbot-Banden, die es auf ukrainische Unternehmen abgesehen haben.

03

Wichtige Statistiken

27 %

Prozentualer Anteil von Angriffen mit Erpressung

Bei mehr als einem Viertel aller Vorfälle, auf die X-Force im Jahr 2022 reagierte, versuchten Bedrohungsakteure, Geld von den Opfern zu erpressen. Ihre Taktiken haben sich in den letzten zehn Jahren weiterentwickelt – ein Trend, der sich voraussichtlich fortsetzen wird, da die Bedrohungsakteure immer aggressiver nach Gewinn streben.

21 %

Anteil der Vorfälle mit Backdoors

Der Einsatz von Backdoors ergab die häufigste Angriffsmethode, die im vergangenen Jahr weltweit bei mehr als einem von fünf gemeldeten Vorfällen angewendet wurde. Der erfolgreiche Einsatz von Abwehrmaßnahmen hat wahrscheinlich verhindert, dass die Bedrohungsakteure weitere Ziele verfolgen konnten, zu denen eventuell auch Ransomware gehört hätte.

17 %

Anteil von Ransomware an Angriffen

Selbst in einem chaotischen Jahr, in dem einige der produktivsten Ransomware-Syndikate aktiv waren, stellte Ransomware die zweithäufigste Angriffsart dar, dicht gefolgt von Backdoor-Bereitstellungen, die auch weiterhin den Geschäftsbetrieb von Unternehmen stören. Der Anteil von Ransomware an den Vorfällen sank von 21 % im Jahr 2021 auf 17 % im Jahr 2022.

41 %

Prozentsatz der Vorfälle, bei denen Phishing für den Erstzugriff eingesetzt wurde
Phishing-Attacken waren auch 2022 die häufigste Art der Angriffe: 41 % der von X-Force bearbeiteten Störfälle nutzten diese Methode für den Erstzugriff.

100 %

Anstieg der Anzahl der Thread-Hijacking-Versuche pro Monat
Im Jahr 2022 gab es doppelt so viele Thread-Hijacking-Versuche pro Monat wie 2021. Thread-Hijacking wurde häufig in Verbindung mit Spam-E-Mails verwendet, die auf Emotet, Qakbot und IcedID zurückzuführen waren.

52 %

Rückgang der gemeldeten Phishing-Kits zur Abfrage von Kreditkartendaten
Fast alle untersuchten Phishing-Kits zielten auf Namen (98 %) und E-Mail-Adressen (73 %) ab, gefolgt von Privatadressen (66 %) und Kennwörtern (58 %). Kreditkartendaten, die 2021 in 61 % der Fälle das Ziel waren, sind bei den Bedrohungsakteuren nicht mehr so beliebt – die Daten zeigen, dass sie 2022 nur noch Ziel von 29 % der Phishing-Kits waren, was einem Rückgang von 52 % entspricht.

62 %

Prozentsatz der Phishing-Attacken mit Spear-Phishing-Anhängen
Die Angreifer bevorzugten den gezielten Einsatz von Anhängen allein oder in Kombination mit Links oder Spear-Phishing als Service.

26 %

Anteil der Schwachstellen 2022 mit bekannten Exploits
26 Prozent der Schwachstellen im Jahr 2022 waren bereits bekannt. Den von X-Force seit Anfang der 1990er-Jahre erfassten Daten zufolge ist dieser Anteil in den letzten Jahren zurückgegangen, was die Vorteile eines gut gepflegten Patch-Management-Prozesses verdeutlicht.

31 %

Anteil der weltweiten Angriffe, die auf den asiatisch-pazifischen Raum abzielten
Der asiatisch-pazifische Raum bleibt auch 2022 die am häufigsten angegriffene Region, auf die 31 % aller Vorfälle entfallen. Dies entspricht einem Anstieg von fünf Prozentpunkten gegenüber dem Gesamtanteil der Angriffe, auf die X-Force im Jahr 2021 in der Region reagiert hat.

Die wichtigsten ursprünglichen Zugriffsvektoren

2022 ging X-Force von der Verfolgung von Erstzugriffsvektoren als breitere Kategorien, wie Phishing und ausgespähte Anmeldedaten, zu Erstzugriffstechniken über, die im Framework der MITRE ATT&CK Matrix for Enterprise aufgeführt sind. Diese Umstellung ermöglicht es X-Force, wichtige Trends auf technischer Ebene genauer zu verfolgen. Darüber hinaus bietet es besser nutzbare und vergleichbare Daten und steht im Einklang mit den Standardisierungsbemühungen der gesamten Branche.

Die wichtigsten ursprünglichen Zugriffsvektoren 2022

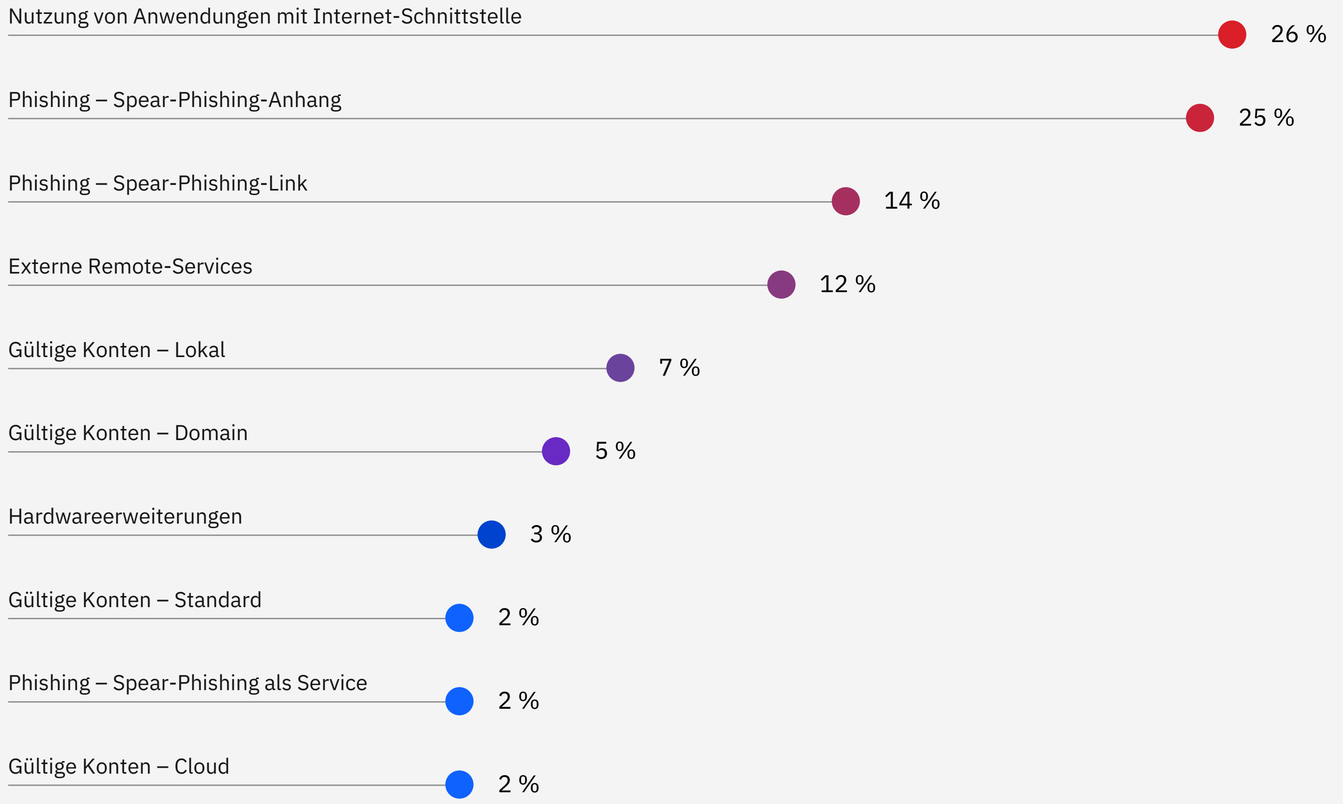


Abbildung 1: Die wichtigsten von X-Force beobachteten ursprünglichen Zugriffsvektoren 2022. Quelle: X-Force

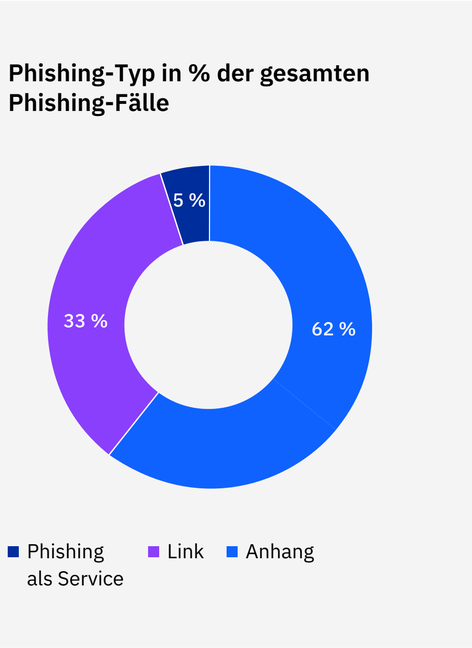


Abbildung 2: Arten von Phishing-Subtechniken in Prozent aller von X-Force beobachteten Phishing-Fälle im Jahr 2022. Quelle: X-Force

Phishing

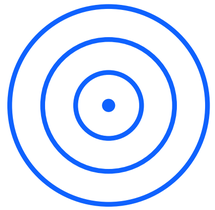
Phishing (T1566), ob durch Anhänge, Links oder als Service, ist nach wie vor der führende Infektionsvektor und machte 2022 41 % aller von X-Force bearbeiteten Vorfälle aus. Dieser Anteil bleibt nach einem Anstieg von 33 % im Jahr 2020 ab 2021 konstant. Betrachtet man alle Phishing-Vorfälle, so wurden bei 62 % der Angriffe Spear-Phishing-Anhänge (T1566.001), bei 33 % Spear-Phishing-Links (T1566.002) und bei 5 % Spear-Phishing-as-a-Service (T1566.003) verwendet. X-Force konnte darüber hinaus beobachten, dass Bedrohungsakteure in einigen Fällen neben Phishing-as-a-Service oder Links auch Anhänge verwenden.

Daten von IBM X-Force Red aus dem Jahr 2022 veranschaulichen den Wert von Phishing und dem falschen Umgang mit Anmeldedaten für Bedrohungsakteure. Bei den Penetrationstests, die X-Force Red 2022 bei Kunden durchführte, wurde bei rund 54 % der Tests eine unsachgemäße Authentifizierung bzw. ein unsachgemäßer Umgang mit Anmeldedaten festgestellt. Das X-Force Red Adversary Simulation Team führte regelmäßig Spear-Phishing-Angriffe mit QR-Codes durch, die auf Token für die Mehrfaktorauthentifizierung (MFA) abzielten. Vielen Unternehmen fehlte die Transparenz über Anwendungen und Endpunkte, auf die über das Identitäts- und Zugriffsmanagement sowie Single-Sign-On- (SSO) Portale wie Okta zugegriffen wurde.

An zweiter Stelle steht die Ausnutzung von Anwendungen mit Internet-Schnittstelle (T1190), d. h. die durch Angreifer verursachte Ausnutzung von Schwachstellen in Computern oder Programmen, die über das Internet zugänglich sind. Sie wurde in 26 % der von der X-Force bearbeiteten Fälle festgestellt. Dies entspricht dem, was in früheren Berichten des Threat Intelligence Index als „Ausnutzung von Schwachstellen“ bezeichnet wurde, und markiert einen Rückgang um 34 % verglichen mit 2021.

An dritter Stelle steht der Missbrauch von gültigen Konten (T1078), der in 16 % der beobachteten Vorfälle festgestellt wurde. In diesen Fällen haben die Angreifer die Anmeldedaten für bestehende Konten ausgespäht und missbraucht, um sich Zugriff zu verschaffe n. Zu diesen Vorfällen gehörten Cloud-Konten (T1078.004) und Standardkonten (T1078.001) mit jeweils 2 %, Domänenkonten (T1078.002) mit 5 % und lokale Konten (T1078.003) mit 7 %.

Rückgang der Angriffe von Phishing-Kits auf Kreditkarteninformationen von 61 % im Jahr 2021 auf 29 % im Jahr 2022.



Phishing-Kits haben eine längere Lebensdauer und zielen eher auf personenbezogene Daten als auf Kreditkartendaten ab

IBM Security hat das zweite Jahr in Folge Tausende von Phishing-Kits aus der ganzen Welt analysiert und festgestellt, dass die Kit-Bereitstellungen länger aktiv sind und mehr Benutzer erreichen. Die Daten zeigen, dass sich die Lebensdauer der beobachteten Phishing-Kits im Vergleich zum Vorjahr mehr als verdoppelt hat, während der Medianwert für die Bereitstellung im gesamten Datensatz mit 3,7 Tagen relativ niedrig blieb.

Insgesamt dauerte die kürzeste Bereitstellung nur wenige Minuten und die längste, die 2022 entdeckt wurde, mehr als drei Jahre. Unsere Untersuchungen ergaben Folgendes:

- Die Einsatzdauer für ein Drittel der bereitgestellten Kits betrug im vergangenen Jahr etwa 2,3 Tage, also mehr als doppelt so lange wie im Jahr zuvor, als der gleiche Anteil nicht länger als einen Tag eingesetzt wurde.
- Etwa die Hälfte aller gemeldeten Kits betraf 93 Benutzer, während 2021 jeder Einsatz durchschnittlich nicht mehr als 75 potenzielle Geschädigte ergab.
- Die maximale Anzahl der Opfer einer gemeldeten Phishing-Attacke lag bei knapp über 4.000, was jedoch einen Ausreißer darstellt.
- Fast alle gemeldeten und analysierten Phishing-Kits versuchten in 98 % der Fälle, Namen abzufassen. Es folgten E-Mail-Adressen mit 73 %, Privatadressen mit 66 % und Kennwörter mit 58 %.
- Kreditkarteninformationen wurden deutlich weniger häufig Ziel von Phishing-Kits. Dieser Anteil fiel von 61 % im Jahr 2021 auf 29 % im Jahr 2022.
- Der Rückgang der Zahl der Phishing-Kits, die auf Kreditkartendaten abzielen, deutet darauf hin, dass sich die Phisher auf personenbezogene Daten (PII) konzentrieren, was ihnen breiter angelegte und gefährlichere Möglichkeiten eröffnet. PII-Daten können entweder gesammelt und im Dark Web oder anderen Foren verkauft oder für weitere Operationen gegen Ziele verwendet werden.

Am meisten von Spoofing betroffene Marken

Zu den Top-Marken, bei denen Spoofing beobachtet wurde, gehören vor allem die größten Namen der Tech-Branche. X-Force geht davon aus, dass diese Veränderung gegenüber der etwas vielfältigeren Liste von 2021 auf die verbesserte Fähigkeit zurückzuführen ist, Marken identifizieren zu können, auf die ein Kit für das Spoofing konfiguriert wurde, und nicht nur jene Marken, auf die es standardmäßig abzielt. Viele Phishing-Kits sind vielseitig einsetzbar und die von Spoofing betroffene Marke kann durch Änderung eines einfachen Parameters ausgetauscht werden. Beispielsweise kann ein Kit, das standardmäßig Gmail fälscht, mit einer geänderten Zeile zu einem Angriff auf Microsoft werden.

Ausgespähte Anmeldedaten zu solchen Services sind wertvoll. Der Zugriff auf Konten, mit denen die Opfer ganze Teile ihrer Online-Präsenz verwalten, kann das Einfallstor für den Zugriff auf andere Konten darstellen. Die Konzentration der Angreifer auf diese Form des Erstzugriffs wird im Cloud Threat Landscape Report 2022 hervorgehoben, der einen mehr als dreifachen Anstieg der Anzahl von Cloud-Konten, die im Dark Web zum Verkauf angeboten werden, auf 200 % im Vergleich zu 2021 feststellt.

Die am meisten von Spoofing betroffenen Marken im Jahresvergleich

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Office365	Hotmail

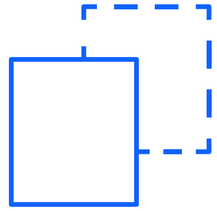
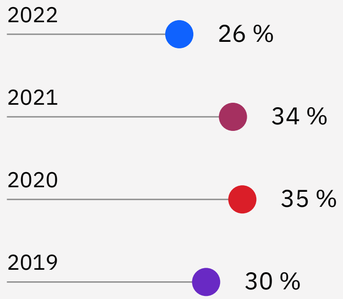


Abbildung 3: Dieses Diagramm zeigt die am häufigsten von Spoofing betroffenen Marken in den Jahren 2021 und 2022 und verdeutlicht, dass sich die Bedrohungsakteure zunehmend auf große Technologiemarken konzentrieren. Quelle: IBM Phishing-Kit-Daten

Anteil der Vorfälle durch Ausnutzung von Schwachstellen in den letzten vier Jahren



Schwachstellen

Die Ausnutzung von Schwachstellen – für 2022 als Ausnutzung von Anwendungen mit Internet-Schnittstelle (T1190) erfasst – steht an zweiter Stelle der wichtigsten Infektionsvektoren und ist seit 2019 eine bevorzugte Kompromittierungsmethode von Angreifern. 2022 nutzten 26 % der von X-Force behobenen Angriffe Schwachstellen aus, ein Jahr zuvor waren es 34 %, im Jahr 2020 35 % und 2019 30 %.

Nicht jede von Bedrohungsakteuren ausgenutzte Schwachstelle führt zu einem Cybervorfall. Die Anzahl der Vorfälle, die auf die Ausnutzung von Schwachstellen zurückzuführen sind, ist 2022 gegenüber 2021 um 19 % zurückgegangen, nachdem sie 2020 um 34 % gestiegen war. X-Force vermutet, dass diese Veränderung auf die weit verbreitete Log4J-Sicherheitslücke Ende 2021 zurückzuführen ist.

Die Ausnutzung des Zugriffs ist ein wichtiger Forschungsbereich, den das Team von X-Force Red Adversary Simulation Services verfolgt, um fortgeschrittene Bedrohungen zu simulieren. Das Team konzentrierte sich verstärkt auf die Untersuchung von Schwachstellen in Betriebssystemen und Anwendungen, die genutzt werden, um Zugriff und Berechtigungen auszuweiten. Dieser Schwerpunkt ergab sich vor allem aus früheren Übungen mit langjährigen Kunden, die die traditionellen Angriffswege von Active Directory abgesichert hatten, sowie aus der Notwendigkeit zur Verfolgung neuer Angriffswege.

Während Sicherheitslücken als gängiges Einfallstor gelten und die Branche jedes Jahr auf mehrere größere reagiert, sind sie nicht immer gleich. Für Entscheidungsträger ist es wichtig, sich einen umfassenden Überblick über die Schwachstellenlandschaft zu verschaffen und sicherzustellen, dass sie über den notwendigen Kontext verfügen, um die tatsächliche Bedrohung zu verstehen, die eine bestimmte Sicherheitslücke für ihre Netzwerke darstellt.

Vor fast 30 Jahren, noch vor der Einführung des CVE-Systems (Common Vulnerabilities and Exposures), begann X-Force mit dem Aufbau einer soliden Schwachstellendatenbank. Diese Datenbank ist heute eine der umfassendsten der Cybersicherheitsbranche. Obwohl Schwachstellen ein großes Sicherheitsrisiko darstellen, gibt es weitaus mehr gemeldete Sicherheitslücken als bekannte und gezielt eingesetzte Exploits. Und trotz der öffentlichen Aufmerksamkeit für Zero Days ist die tatsächliche Anzahl bekannter Zero Days im Vergleich zur Gesamtzahl bekannter Schwachstellen verschwindend gering.

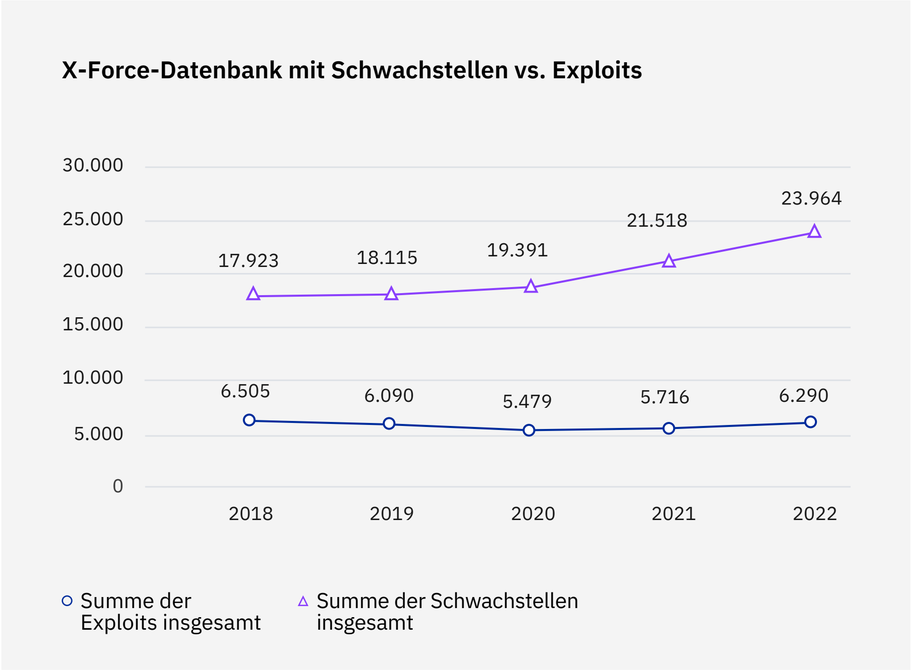


Abbildung 4: X-Force-Schwachstellendatenbankansicht mit Sicherheitslücken und Exploits der letzten fünf Jahre. Quelle: X-Force

Jedes Jahr wird eine neue Rekordzahl an Sicherheitslücken entdeckt. Die Gesamtzahl der 2022 erfassten Sicherheitslücken belief sich auf 23.964 gegenüber 21.518 im Jahr 2021. Dieser Zunahmetrend hat sich in den letzten zehn Jahren von Jahr zu Jahr fortgesetzt. Die Analyse unserer Schwachstellendatenbank hat ergeben, dass das Verhältnis zwischen bekannten, funktionsfähigen Exploits und den gemeldeten Schwachstellen in den letzten Jahren abgenommen hat: 36 % im Jahr 2018, 34 % im Jahr 2019, 28 % im Jahr 2020, 27 % im Jahr 2021 und 26 % im Jahr 2022.

Diese Zahlen können sich ändern, wenn Zero Days und Exploits für ältere Schwachstellen entwickelt werden – was manchmal erst Jahre nach ihrer Entdeckung der Fall ist. Für diesen Rückgang gibt es mehrere mögliche Erklärungen. Erstens hat die Einführung formeller Bug-Bounty-Programme Anreize für die proaktive Entdeckung von Schwachstellen in Anwendungen geschaffen. Darüber hinaus gibt es einige weit verbreitete und etablierte Schwachstellen, die Angreifern bereits als Mittel zur Ausnutzung von Systemen dienen, sodass die Bedrohungsakteure keine neuen Exploits entwickeln müssen. Dieser Rückgang ist wahrscheinlich auf eine Kombination aus mehreren Faktoren zurückzuführen, deutet aber nicht darauf hin, dass die Ausnutzung von Schwachstellen weniger bedrohlich geworden ist.

Während das Verhältnis von Exploits zu Schwachstellen kleiner wird, hat der Schweregrad der von X-Force erfassten Exploits in den letzten fünf Jahren zugenommen. 58 % der Schwachstellen hatten 2018 einen mittleren Wert (Common Vulnerability Scoring System, CVSS),

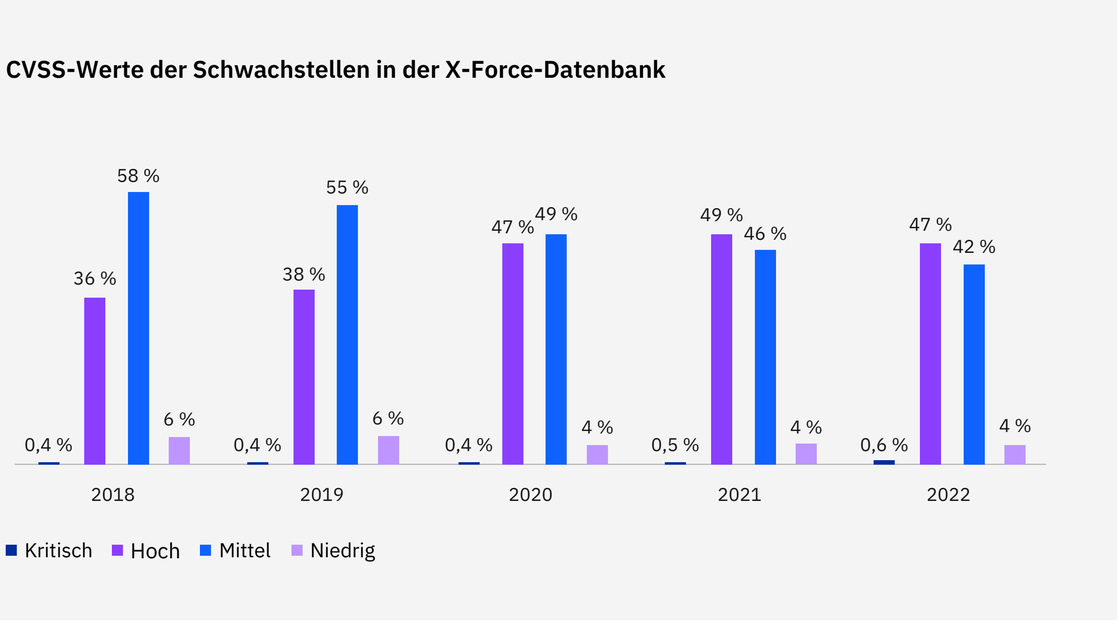


Abbildung 5: X-Force-Schwachstellendatenbank mit Schweregrad der in unserem System erfassten Sicherheitslücken. Quelle: X-Force

4,0–6,9 von 10, verglichen mit knapp 36 %, die auf 7,0–9,9 kamen. Im Jahr 2021 hat sich die Verteilung zwischen diesen beiden Werten umgekehrt. Die Schwachstellen mit hohem Schweregrad machen jetzt fünf Prozentpunkte mehr aus als die mit mittlerem Schweregrad.

Von allen Schwachstellen, die X-Force seit 1988 erfasst hat, werden 38 % als hoch eingestuft, wohingegen nur 1 % den kritischen Wert von 10 erreicht. Die Hälfte der ermittelten Schwachstellen wird als mittel eingestuft, die restlichen 11 % als niedrig bei 3,9 und darunter. Diese Werte allein spiegeln nicht den tatsächlichen Schweregrad eines CVE wider, da sie nicht berücksichtigen, wie die Schwachstelle ausgenutzt wird oder ob überhaupt ein Exploit vorliegt. Die Bewertungen helfen den Sicherheitsexperten jedoch, Schwachstellen zu vergleichen und zu deren schnelleren Behebung Prioritäten zu setzen. Die Grafik in Abbildung 6 auf der folgenden Seite verdeutlicht das wahre Ausmaß des Schwachstellenproblems in der Cybersicherheitsbranche.

Schwachstellen der Betriebstechnik (OT)

Die Anzahl der 2022 entdeckten Schwachstellen in industriellen Steuersystemen (ICS) ist zum ersten Mal seit zwei Jahren zurückgegangen: auf 457 im Jahr 2022 gegenüber 715 im Jahr 2021 und 472 im Jahr 2020. Die Lebenszyklen von ICS und die Art und Weise, wie sie im Allgemeinen verwaltet und gepatcht werden, könnten eine Erklärung dafür sein. Angreifer wissen, dass viele ICS-Komponenten und OT-Netzwerke aufgrund der Forderung nach minimalen Ausfallzeiten, langen Gerätelebenszyklen und älterer, weniger unterstützter Software immer noch durch ältere Schwachstellen gefährdet sind. Die Infrastruktur ist in der Regel viele Jahre länger in Betrieb als herkömmliche Büro-Workstations, was die Lebensdauer von ICS-spezifischen Schwachstellen über die von IT-Schwachstellen hinaus verlängert.

Das Problem mit den Schwachstellen

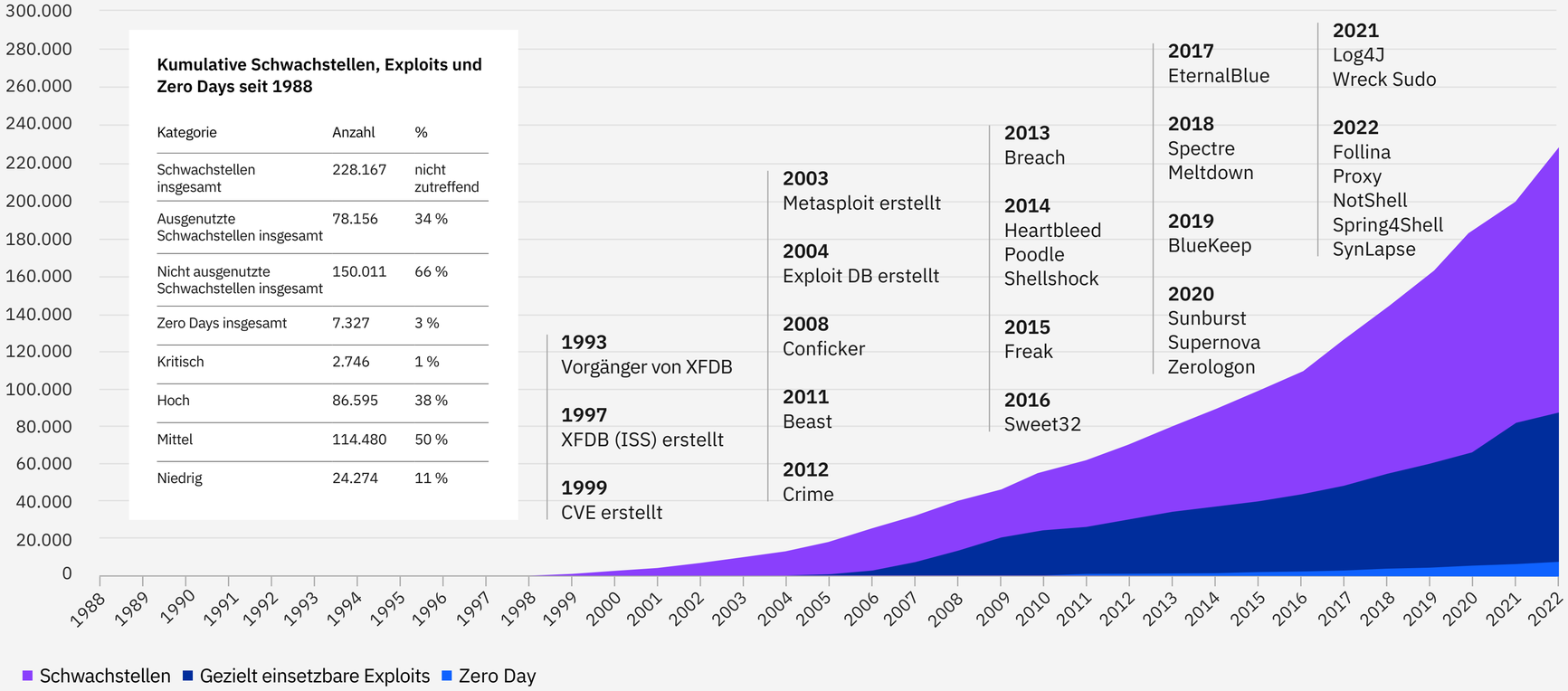


Abbildung 6: Die Grafik zeigt die Zunahme von Schwachstellen, Exploits und Zero Days seit 1988. Außerdem eine Zeitleiste der wichtigsten Ereignisse im Zusammenhang mit Schwachstellen seit 1993. XFDB steht für X-Force Database und Exploit DB steht für Exploit Database. Quelle: X-Force

Die wichtigsten Angriffsmethoden

Zuvor wurde im X-Force Threat Intelligence Index die breite Kategorie der wichtigsten Angriffe untersucht. Für 2022 hat X-Force diese Klassifizierung in zwei verschiedene Kategorien unterteilt: die spezifischen Handlungen der Bedrohungsakteure in den Netzwerken der Opfer oder die Angriffsmethoden sowie die beabsichtigten oder realisierten Auswirkungen dieser Handlungen auf das Opfer oder die Folgen.

Aus den Daten von X-Force Incident Response geht hervor, dass die Verwendung von Backdoors mit einem Anteil von 21 % an allen gemeldeten Vorfällen die häufigste Angriffsmethode darstellte. Es folgten Ransomware mit 17 % und die Kompromittierung geschäftlicher E-Mails (BEC) mit 6 %. Schädliche Dokumente (Maldocs), Spamkampagnen, Fernzugriffstools und Serverzugriff wurden in jeweils 5 % der Fälle entdeckt.

Die wichtigsten Angriffsmethoden 2022

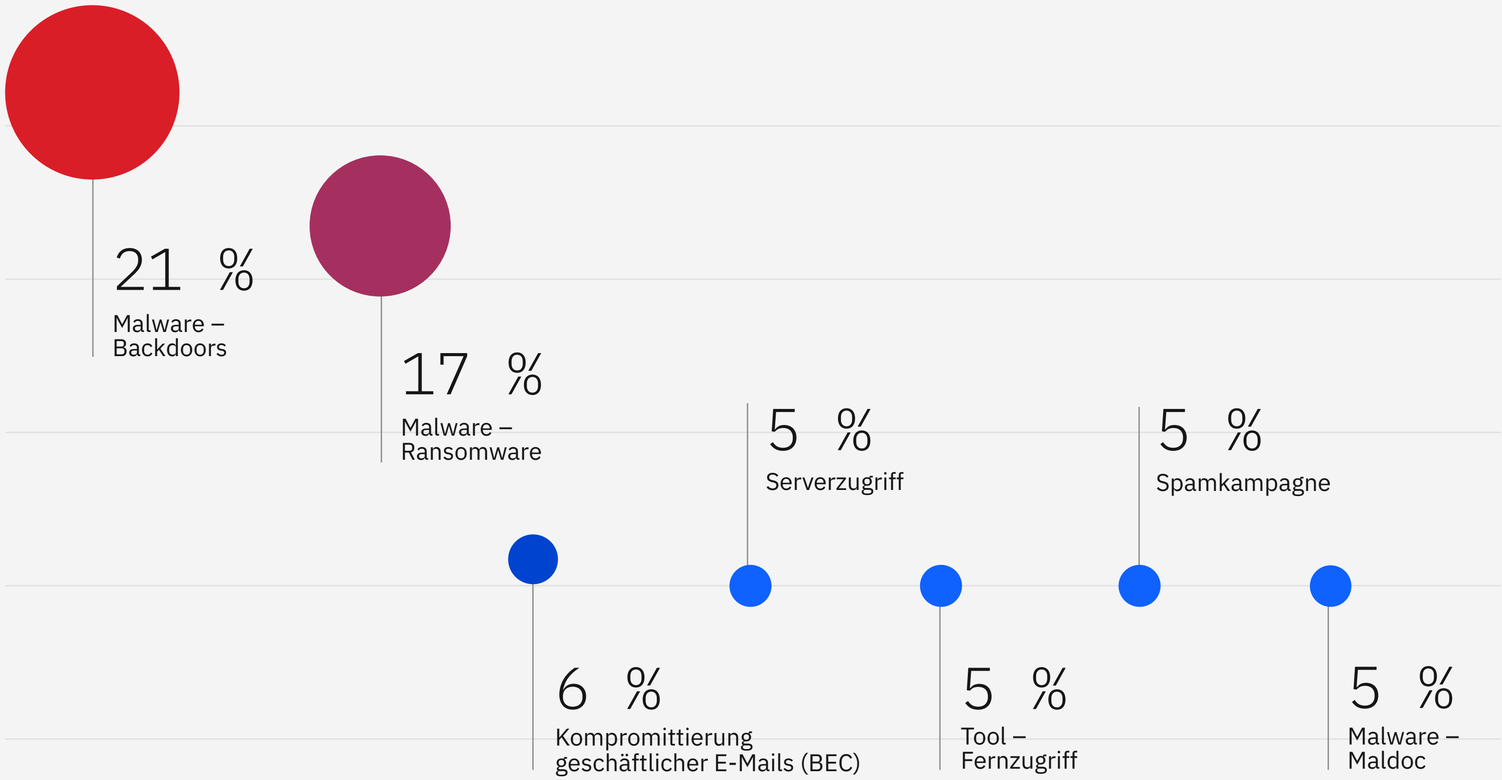


Abbildung 7: Die wichtigsten von X-Force beobachteten Angriffsmethoden im Jahr 2022. Quelle: X-Force

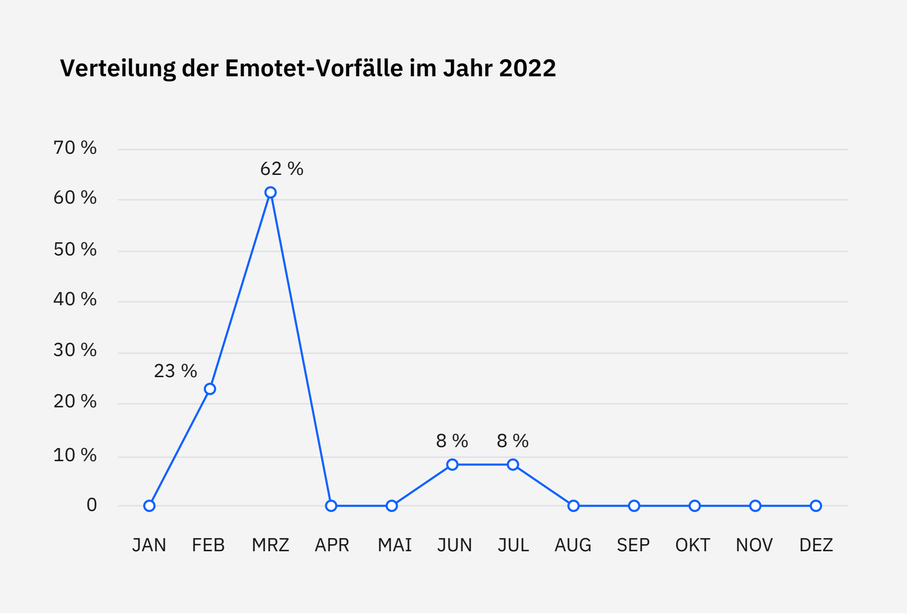


Abbildung 8: Die Grafik zeigt den sprunghaften Anstieg der Emotet-Fälle zu Beginn des Jahres 2022. Quelle: X-Force

In Fällen, in denen eine Backdoor-Bereitstellung als Angriffsmethode eingestuft wurde, ist es wahrscheinlich, dass der Bedrohungsakteur weitere Pläne hatte, wenn die Backdoor in Betrieb genommen wurde. Ein erfolgreiches Eingreifen der Sicherheitsteams oder des Teams zur Fehlerbehebung hat wahrscheinlich verhindert, dass der Bedrohungsakteur weitere Ziele erreichen konnte. Zu diesen weiteren böswilligen Aktivitäten gehörte wahrscheinlich auch Ransomware, da etwa zwei Drittel dieser Backdoor-Fälle die Merkmale einer Ransomware-Attacke aufwiesen.

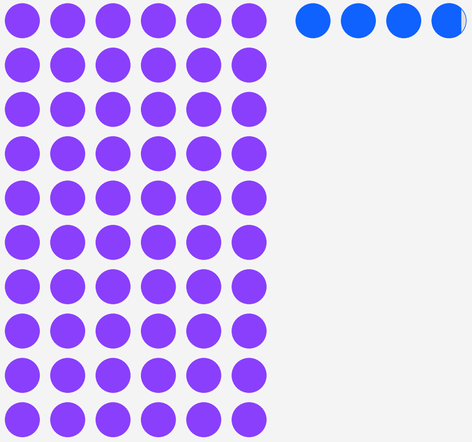
Der vermehrte Einsatz von Backdoors könnte auch auf den Gewinn zurückzuführen sein, der sich mit dieser Art des Zugriffs im Dark Web erwirtschaften lässt. Ein kompromittierter Zugriff zum Unternehmensnetzwerk von einem Initial Access Broker kostet in der Regel mehrere Tausend US-Dollar. Mit dieser Art des Zugriffs können böswillige Akteure, die einen schnellen Gewinn erzielen wollen, Probleme bei der Aufrechterhaltung des Zugriffs vermeiden, während sie mit der Bedrohung in die Breite gehen und wertvolle Daten exfiltrieren. Böswillige Akteure, die nicht über die erforderliche Malware verfügen, um sich selbst Zugriff zu verschaffen, können dies auch über Backdoors versuchen.

Inital Access Broker versuchen in der Regel, ihre Zugänge zu versteigern, wobei X-Force Preise von 5.000 bis 10.000 USD beobachten konnte. Jedoch können die Endpreise auch niedriger sein. Andere berichten von Zugängen, die für 2.000 bis 4.000 USD verkauft werden, einer sogar für 50.000 USD. Diese Beträge stehen den deutlich niedrigeren Preisen für eine einzelne Kreditkarte gegenüber, die für weniger als 10 USD angeboten wird.

Backdoors führten im Februar und März zu einem bemerkenswerten Anstieg der Emotet-Fälle. Dieser Anstieg hat die Rangliste der Backdoor-Fälle erheblich beeinflusst, da die in diesem Zeitraum installierten Backdoors 47 % aller 2022 weltweit identifizierten Backdoors ausmachten. Nach einer Pause von Emotet von Juli bis November – nach der es fast zwei Wochen lang mit deutlich geringerem Volumen wieder hochgefahren wurde – ging die Zahl der Backdoor-Fälle deutlich zurück.

Durchschnittliche Dauer von Ransomware-Attacken

2019	2021
Über 2 Monate	Über 3 Tage



Ransomware

Selbst in einem chaotischen Jahr, in dem einige der produktivsten Ransomware-Syndikate aktiv waren, stellte Ransomware die zweithäufigste Angriffsart dar, dicht gefolgt von Backdoor-Bereitstellungen, die auch weiterhin den Geschäftsbetrieb von Unternehmen stören. Der Anteil von Ransomware an den Vorfällen sank von 21 % im Jahr 2021 auf 17 % im Jahr 2022.

Eine IBM Security X-Force-Studie ergab, dass die durchschnittliche Dauer von Ransomware-Attacken von 2019 bis 2021 um 94,34 % von über zwei Monaten auf knapp vier Tage gesunken ist. Dennoch stellt Ransomware eine eindeutige und allgegenwärtige Bedrohung dar, und es gibt Anzeichen dafür, dass sie sich eher weiter ausbreitet als nachlässt.

Besonders schädigend ist die Verbreitung von Schadteilen durch Ransomware über ein Netzwerk, wenn dabei Domänencontroller kompromittiert werden. Bei einem kleinen Prozentsatz der von X-Force Red durchgeführten Netzwerk-Penetrationstests (ca. 4 %) wurden Unternehmen mit fehlerhaften Konfigurationen im Active Directory gefunden, was zu einer Ausweitung der Berechtigungen oder zur vollständigen Übernahme der Domäne führen konnte. Im Jahr 2022 beobachtete X-Force auch aggressivere Ransomware-Attacken auf die zugrunde liegende Infrastruktur, wie ESXi und Hyper-V. Die potenziell weitreichenden Auswirkungen dieser Angriffsmethoden machen deutlich, wie wichtig es ist, Domänencontroller und Hypervisoren angemessen zu schützen.

Ransomware-Varianten

Da sich Ransomware-Gruppen und die jeweiligen Zugriffsbroker ständig ändern, konnte X-Force regelmäßige Veränderungen bei den führenden Gruppen feststellen, die in diesem Bereich aktiv sind. X-Force hat 2022 19 Varianten von Ransomware entdeckt, verglichen mit 16 im Jahr 2021. LockBit-Varianten machten 17 % der insgesamt beobachteten Ransomware-Vorfälle aus, gegenüber 7 % im Jahr 2021. Phobos lag mit 11 % an zweiter Stelle gleichauf mit WannaCry. Die führenden Gruppen im Jahr 2022 verdrängten den Erstplatzierten des Jahres 2021, REvil, auch bekannt als Sodinokibi, mit 37 % der Fälle im Jahr 2021 und den Zweitplatzierten Ryuk mit 13 %, die beide auf 3 % zurückfielen.

LockBit 3.0 ist die neueste Variante der Ransomware-Familie LockBit und Teil einer Ransomware-as-a-Service (RaaS)-Operation, die mit LockerGoga und MegaCortex in Verbindung steht. LockBit ist seit September 2019 aktiv, und LockBit 3.0 kam 2022 heraus. Ein wesentlicher Teil des Quellcodes von LockBit 3.0 scheint von der Ransomware BlackMatter übernommen worden zu sein.

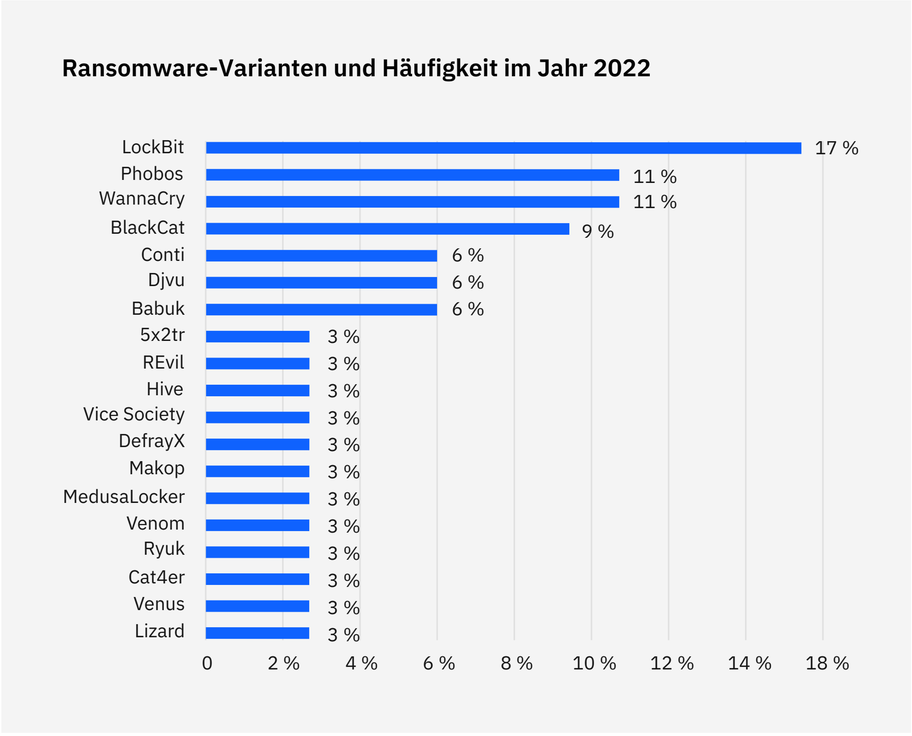


Abbildung 9: Ransomware-Varianten und die Häufigkeit, mit der sie bei Aktivitäten von X-Force Incident Response 2022 beobachtet wurden. Quelle: X-Force

Forscher entdeckten die Ransomware Phobos erstmals Anfang 2019. Aufgrund von Ähnlichkeiten im Code, der Verbreitungsmechanismen, der Angriffstechniken und der Erpressungsnachrichten wurde Phobos als Variante der bereits bekannten Ransomware-Familien Crysis und Dharma identifiziert. Phobos wurde häufig für kleinere Angriffe mit geringeren Lösegeldforderungen eingesetzt. E-Mail-Phishing-Kampagnen und das Ausnutzen anfälliger RDP-Ports (Remote Desktop Protocol) sind die wichtigsten Verbreitungswege von Phobos.

WannaCry tauchte erstmals 2017 auf und verbreitet sich selbst, indem es mithilfe von EternalBlue die Sicherheitslücke im Microsoft Server Message Block 1.0 (SMBv1) Server (MS17-010) ausnutzt. Mehrere Fälle von WannaCry oder Ryuk, die X-Force 2022 beobachtete, waren das Ergebnis von Infektionen, die drei bis fünf Jahre zurücklagen und auf alten, ungepatchten Geräten auftraten, was die Wichtigkeit einer ordnungsgemäßen Bereinigung nach solchen Ereignissen unterstreicht.

Kompromittierung geschäftlicher E-Mails (BEC)

BEC liegt 2022 mit 6 % der Vorfälle, auf die X-Force reagiert hat, wieder auf dem dritten Platz. Der Prozentsatz ist etwas niedriger als die 8 % der Angriffe 2021 und die 9 % für den fünften Platz 2020. Er verdrängte den zweitplatzierten Angriff von 2021, bei dem es sich um Angriffe auf Server handelte. Bei dieser Art von Angriffen verschafft sich ein Angreifer mit unbekanntem Ziel Zugang zu einem Server. Im Jahr 2022 wurde diese Art von Angriffen genauer danach klassifiziert, welche Art von Zugang diese Akteure erreicht haben. In der Hälfte der BEC-Fälle, auf die X-Force reagierte, wurden Spear-Phishing-Links verwendet. In jeweils 25 % der Fälle wurden schädliche Anhänge genutzt und gültige Konten für BEC-Versuche missbraucht.

06

Die wichtigsten Auswirkungen

X-Force untersuchte auch die Folgen der Vorfälle für die betroffenen Unternehmen, um besser zu verstehen, welche Auswirkungen die Bedrohungsakteure mit den Vorfällen, auf die X-Force reagierte, erzielen wollten. Anhand dieser Informationen können die Unternehmen die häufigsten Auswirkungen besser verstehen und Reaktionen auf mögliche zukünftige Vorfälle effektiver planen.

Die Analyse ergab, dass mehr als einer von vier Vorfällen darauf abzielte, das betroffene Unternehmen zu erpressen – dies war die häufigste Auswirkung der von X-Force behobenen Vorfälle. Die beobachteten Erpressungsfälle wurden meist mithilfe von Ransomware oder BEC durchgeführt und beinhalteten häufig den Einsatz von Fernzugriffstools, Cryptominern, Backdoors, Downloadern und Web Shells.

Die wichtigsten Auswirkungen 2022

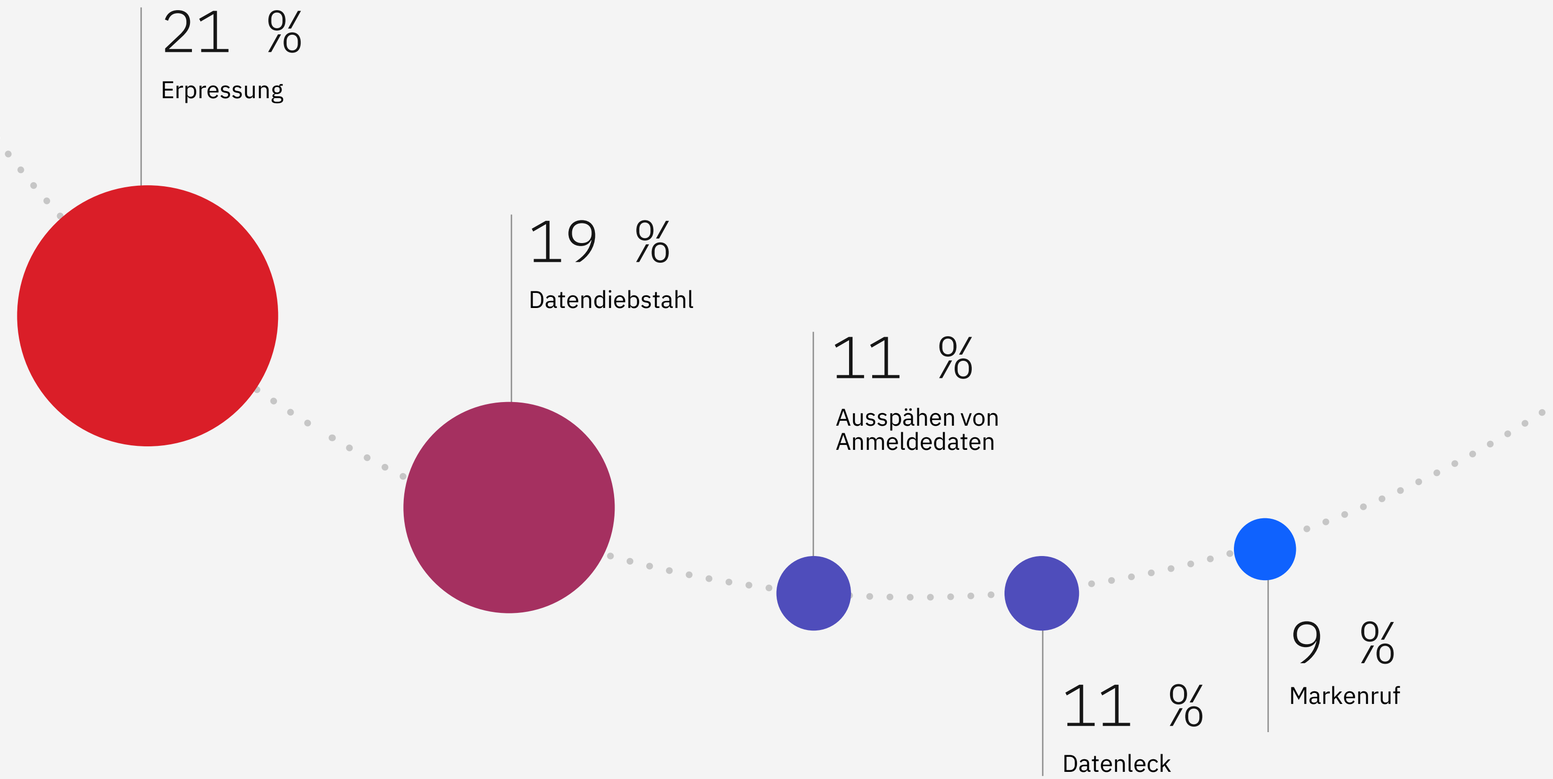


Abbildung 10: Die wichtigsten Auswirkungen, die X-Force bei Incident-Response-Aktivitäten 2022 beobachtet hat. Quelle: X-Force

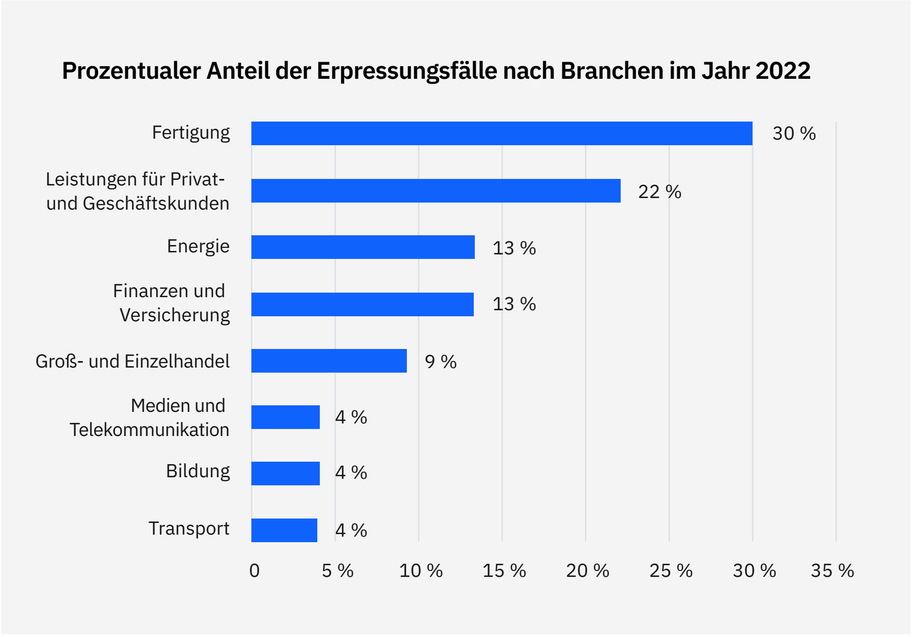


Abbildung 11: Der prozentuale Anteil der Erpressungsfälle, die X-Force im Rahmen von Incident-Response-Einsätzen 2022 beobachtet hat. Die Summe der Zahlen ergibt aufgrund von Rundungen nicht 100 %. Quelle: X-Force

An zweiter Stelle stand Datendiebstahl, der 19 % aller von X-Force behobenen Vorfälle ausmachte. Das Ausspähen von Anmeldedaten, bei dem Benutzernamen und Kennwörter entwendet wurden und entsprechende Abhilfemaßnahmen erforderlich wurden, beliefen sich auf 11 %. Vorfälle, bei denen X-Force gezielte Informationen identifizieren konnte, die nach dem Diebstahl tatsächlich weitergegeben wurden, waren mit 11 % weniger häufig als Datendiebstahl. Auswirkungen auf den Markenruf, wie z. B. die Beeinträchtigung der Services, die Unternehmen ihren Kunden anbieten, machten 9 % der Vorfälle aus. Im Anhang findet sich eine vollständige Liste der von X-Force erfassten Auswirkungen. Bei den Vorfällen, die sich auf den Markenruf des Opfers auswirkten, handelte es sich hauptsächlich um DDoS-Attacken (Distributed Denial of Service), die häufig auch zur Erpressung der Opfer genutzt werden, damit diese Geld zahlen, um den Angriff zu stoppen.

Bemerkenswerte Entwicklungen bei der Online-Erpressung[1–9]

Jahr	Ereignis	Taktik
2013	Cryptolocker – eine der ersten großen Wellen von Ransomware	Datenverschlüs-selung
2014	DDoS 4 Bitcoin, Armada Collective	Ransom DDoS
2015	Chimera-Ransomware erhöht die Gefahr, dass gestohlene Daten online weitergegeben werden	Doppelerpressung
2017–18	BitPaymer und SamSam	Big Game Hunting
2020	Vastaamo-Ransomware	Dreifacherpressung

Erpressung

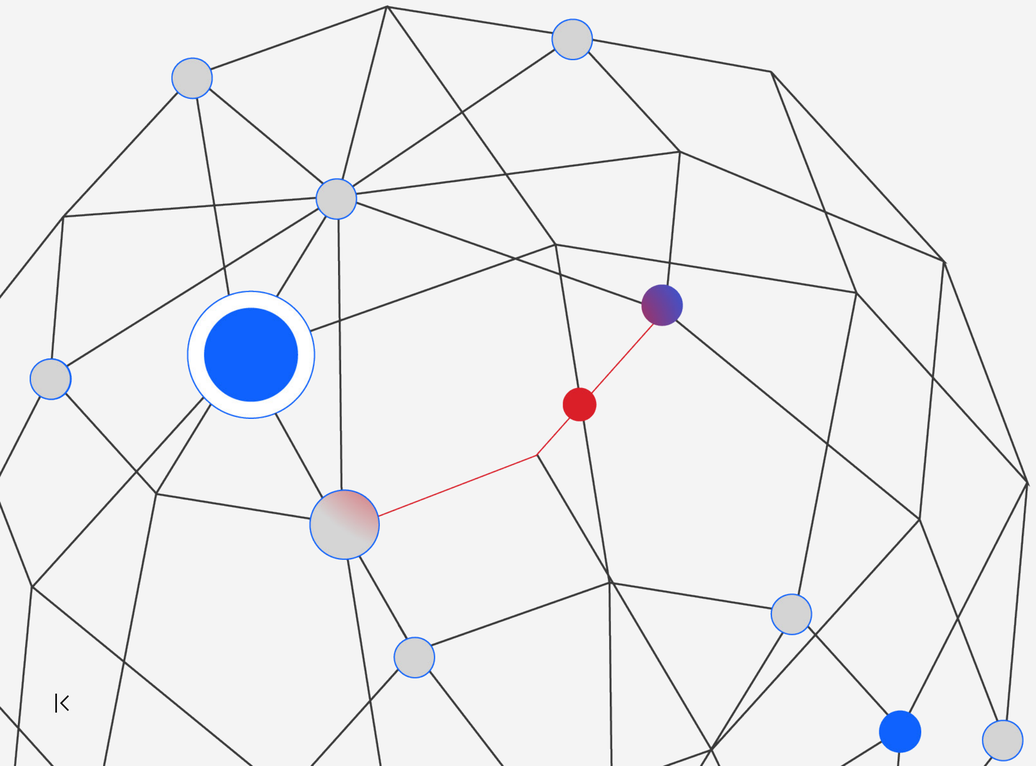
Obwohl Erpressung heute meist mit Ransomware in Verbindung gebracht wird, wird bei Erpressungskampagnen eine Vielzahl an Methoden eingesetzt, um Druck auf die Opfer auszuüben. Dazu gehören DDoS-Bedrohungen, Datenverschlüsselung und neuerdings auch Doppel- und Dreifach-Erpressungen, bei denen mehrere bereits bekannte Elemente kombiniert werden.

Eine weitere Taktik, mit der mindestens eine Ransomware-Gruppe ab 2022 experimentierte, bestand darin, die gestohlenen Daten für nachfolgende Opfer zugänglicher zu machen. Bei dieser Taktik wird es den Opfern aus der zweiten Reihe einfach gemacht, ihre Daten in einem Datenleck zu identifizieren. Somit soll der Druck auf das Unternehmen erhöht werden, welches die Ransomware-Gruppe oder die dazugehörige Gruppe ins Visier genommen hat. X-Force geht davon aus, dass Bedrohungsakteure bis 2023 mit erweiterten oder neuartigen nachgelagerten Benachrichtigungen der Opfer experimentieren werden, um potenzielle juristische Kosten und Rufschädigung eines Angriffs zu erhöhen.

Häufig konzentrieren sich sowohl die Sicherheitsexperten als auch die Opfer von Cyberattacken in erster Linie auf die von den Bedrohungsakteuren beobachteten Auswirkungen auf ein Unternehmen. Es ist jedoch ebenso wichtig, die Absichten und Fähigkeiten der Bedrohungsakteure zu untersuchen und zu beobachten, wie sich diese im Laufe der Zeit verändern und weiterentwickeln. Mit diesem Ansatz lässt sich besser feststellen, wohin die Weiterentwicklung dieser Fähigkeiten in Zukunft führen könnte. Erpressungsmöglichkeiten erweitern sich ständig, wobei das primäre Ziel der Ransomware-Akteure darin liegt, finanzielle Gewinne zu erzielen. Daher geht das X-Force-Team davon aus, dass die Bedrohungsakteure ihre Erpressungsmethoden weiterentwickeln und stets neue Wege finden werden, um Opfer zu Zahlungen zu zwingen.

07

Cyber-bezogene Entwicklungen im Zusammenhang mit dem Krieg Russlands in der Ukraine



Die staatlich geförderten Cyberaktivitäten Russlands nach der russischen Invasion in der Ukraine haben zum Zeitpunkt der Veröffentlichung dieses Berichts nicht zu den weit verbreiteten und folgenschweren Angriffen geführt, die westliche Regierungsstellen ursprünglich befürchtet hatten. Russland hat jedoch eine noch nie dagewesene Anzahl von Wiper-Angriffen gegen Ziele in der Ukraine eingesetzt, was seine anhaltenden Investitionen in zerstörerische Malware verdeutlicht. Darüber hinaus hat die Invasion zu einem Wiederaufleben hacktivistischer Aktivitäten von Gruppen geführt, die mit einer der beiden Seiten sympathisieren, sowie zu einer Neuordnung der cyberkriminellen Landschaft in Osteuropa.

Angesichts der seit 2015 zu beobachtenden fortgeschrittenen Fähigkeiten Russlands bei der Durchführung von Cyberattacken auf kritische Infrastrukturen haben die internationalen Behörden für Cybersicherheit im April 2022 eine Warnung herausgegeben. In der Warnung wurde auf potenziell signifikante Cyberoperationen und damit verbundene Störungen sowohl in der Ukraine als auch in anderen Ländern hingewiesen. X-Force bewertete die wichtigsten Bedrohungen, einschließlich der Rückkehr von Hacktivismus und Wiper-Malware, sowie die wichtigsten Veränderungen in der Welt der Cyberkriminellen. Die meisten dieser Operationen betrafen Einrichtungen in der Ukraine, in Russland und in den Nachbarländern, aber einige haben sich auch auf andere Gebiete ausgeweitet.

Alternativ machen sich Sicherheitsexperten auf geschickte Art und Weise die Fortschritte zunutze, die in den letzten Jahren in den Bereichen Erkennung, Reaktion und Informationsaustausch erzielt wurden. Viele der ersten Angriffsversuche durch Wiper wurden schnell identifiziert, analysiert und publik gemacht. Zu diesen Angriffen zählen mindestens acht identifizierte Wiper-Angriffe sowie die Entdeckung und Unterbrechung einer geplanten russischen Cyberattacke auf das ukrainische Stromnetz im April 2022.

Im Cyberspace sind die Auswirkungen des aktuellen Krieges vor allem durch selbst ernannte Hacktivistengruppen zu spüren, die sich für die nationalen Interessen der Ukraine oder Russlands stark machen. Während sich seit der russischen Invasion viele Gruppen gebildet haben, die sowohl gegen russische als auch ukrainische Netzwerke zur Erreichung politischer Ziele vorgehen, hebt sich Killnet als eine der produktivsten pro-russischen Gruppen hervor. Sie hat DDoS-Attacken auf öffentliche Einrichtungen, Ministerien, Flughäfen, Banken und Energieunternehmen in den Mitgliedstaaten der NATO, in verbündeten Ländern in Europa sowie in Japan und den Vereinigten Staaten durchgeführt. Unternehmen, auf die das Zielprofil von Killnet zutrifft, sollten sicherstellen, dass Maßnahmen zur DDoS-Abwehr ergriffen werden, z. B. durch die Beauftragung eines Drittanbieters zur DDoS-Abwehr.

Zeitleiste ausgewählter Hacktivismus-Ereignisse 2022

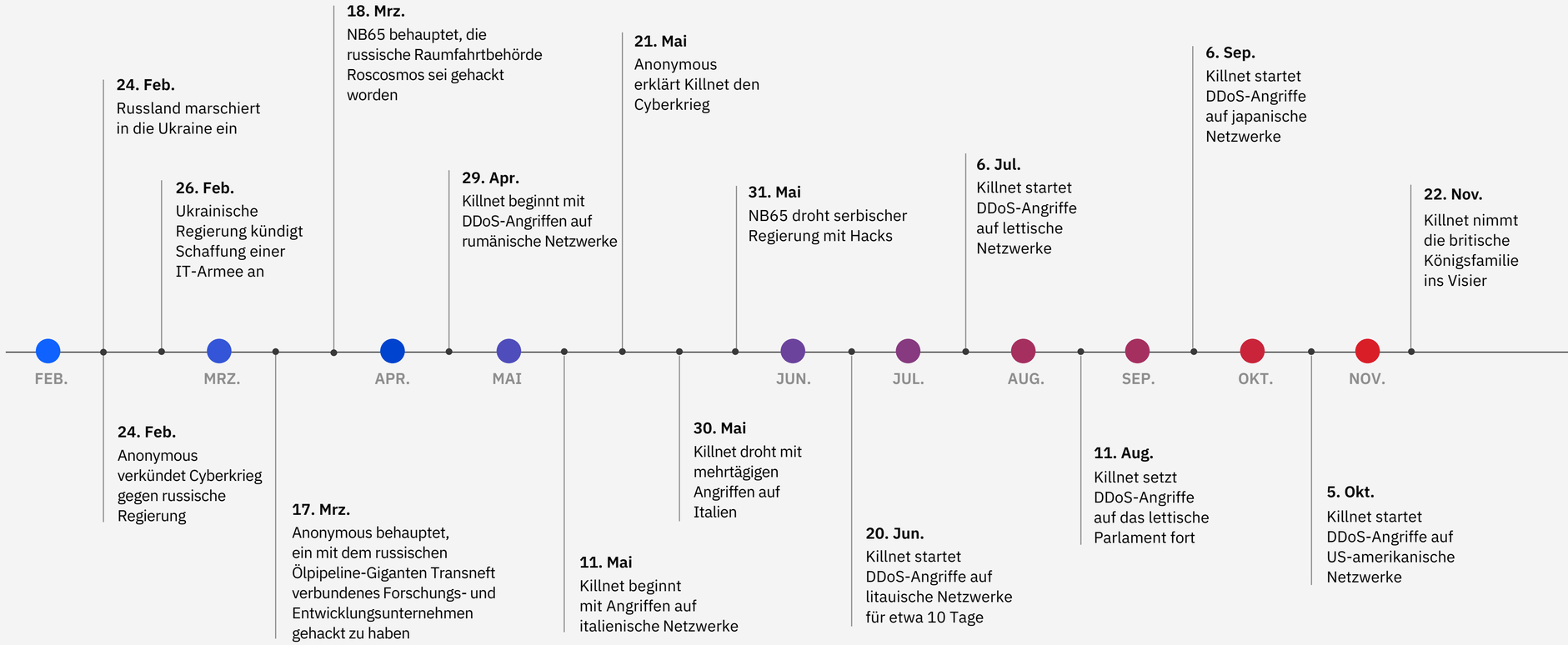


Abbildung 12: Das Bild zeigt die bisher beobachteten Hacktivismus-Ereignisse während des Konflikts in der Ukraine. Quelle: X-Force-Analyse von Open-Source-Berichten

Verwendung von Wipers in Russlands Krieg in der Ukraine

Russlands Krieg in der Ukraine zeichnet sich durch den Einsatz mehrerer Wiper-Familien aus, die in rascher Folge und in beispiellosem Ausmaß gegen mehrere Ziele eingesetzt wurden, sowie durch den Einsatz von Malware neben kinetischen Militäroperationen.

Hierzu gehören mindestens neun neue Wiper: AcidRain, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AwfulShred, OrcShred und SoloShred. Diese Wiper-Angriffe wurden vor allem gegen ukrainische Netzwerke in der Zeit vor der Invasion und in der Anfangsphase des Krieges, hauptsächlich von Januar bis März 2022, eingesetzt. Während es bereits in der Vergangenheit zum Einsatz von Wipers kam, handelte es sich dabei jedoch meist um eigenständige Kampagnen gegen eine begrenzte Anzahl von Zielen.

Die bemerkenswerten Ausnahmen WannaCry und NotPetya, die sich wahllos ausbreiteten, nachdem sie ihre ersten Opfer getroffen hatten, lassen allerdings befürchten, dass sich solche Wiper entweder weiter verbreiten oder für böswillige Operationen an anderer Stelle wiederverwendet werden.

X-Force geht weiterhin davon aus, dass vom russischen Staat gesponserte Cyberbedrohungsakteure nach wie vor eine erhebliche Bedrohung für Computernetze und kritische Infrastrukturen auf der ganzen Welt darstellen. Diese Einschätzung basiert auf langjährigen russischen Cyberoperationen, die auf ukrainische, europäische, NATO- und US-Netzwerke abzielen, sowie auf Angriffsoperationen, die von russischen Bedrohungsgruppen seit 2015 durchgeführt werden.

Unruhe bei russischen cyberkriminellen Gruppen

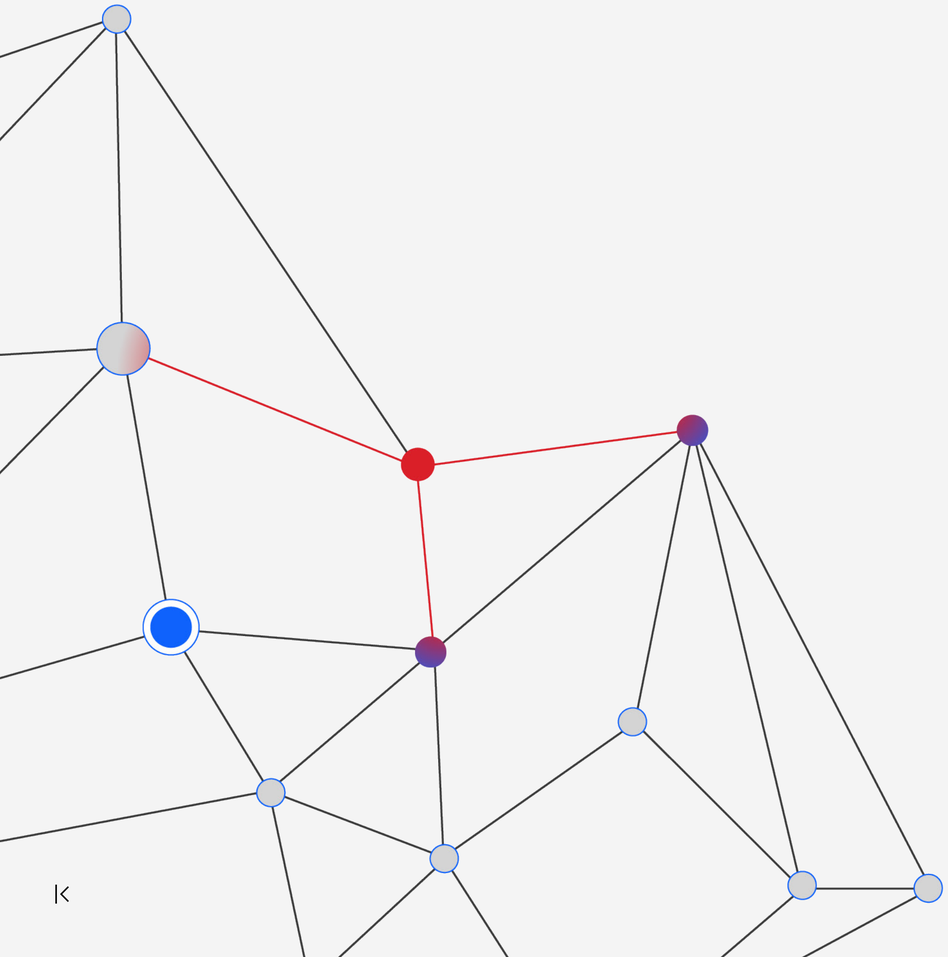
2022 war ein turbulentes Jahr für ITG23 – eines der bekanntesten russischen Cyberkriminellen-Syndikate, das vor allem für die Entwicklung des Banking-Trojaners Trickbot und der Ransomware Conti bekannt ist. Anfang 2022 war die Gruppe von einer Reihe von Lecks betroffen, nachdem sie Russlands Krieg öffentlich befürwortet hatte. Sogenannte ContiLeaks und TrickLeaks führten zur Veröffentlichung tausender Chatnachrichten und zur Enttarnung zahlreicher Gruppenmitglieder. X-Force fand Beweise dafür, dass ITG23 von Mitte April bis mindestens Mitte Juni 2022 systematische Angriffe durchführte – eine beispiellose Entwicklung, da die Gruppe zuvor nicht gegen die Ukraine vorgegangen war.

Darüber hinaus hat die Gruppe offenbar die Nutzung von zwei ihrer bekanntesten Malware-Familien, Trickbot und Bazar, aufgegeben und ihre Conti-Ransomware-Operation eingestellt. Verschiedene Berichte deuten darauf hin, dass es zu einer erheblichen personellen Umstrukturierung kommen könnte, bei der sich die Gruppe in mehrere Fraktionen aufspaltet und einige Mitglieder ganz ausscheiden.

Mit dem Ende der Nutzung von Trickbot und Bazar, die im Jahr 2021 für eine beträchtliche Anzahl von Infektionen verantwortlich waren, öffnete sich eine Lücke, die schnell von Malware-Familien wie Emotet, IcedID, Qakbot und Bumblebee gefüllt wurde. Vor seiner Einstellung verbreitete ITG23 weiterhin Conti-Ransomware und war für ein Drittel aller Ransomware-Aktionen verantwortlich, auf die X-Force im ersten Quartal 2022 reagierte.

Die Gruppe veröffentlichte außerdem eine neue Version ihrer Anchor-Malware, einer getarnten Backdoor, die sie traditionell gegen bedeutende Ziele einsetzt. Die von X-Force entdeckte aktualisierte Version mit dem Namen AnchorMail verfügt über einen neuartigen E-Mail-basierten Kommunikationsmechanismus für die Befehls- und Kontrollfunktion (C2). Der C2-Server verwendet die Protokolle Simple Mail Transfer Protocol Secure (SMTPS) und Internet Message Access Protocol Secure (IMAPS). Die Malware kommuniziert mit dem Server, indem sie speziell gestaltete E-Mail-Nachrichten sendet und empfängt.

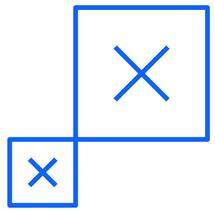
Die Malware-Landschaft



Zunahme der sich über USB verbreitenden Würmer

Nachdem X-Force Mitte Mai 2022 Infektionsversuche mit Raspberry Robin in Unternehmen beobachtet hatte, verbreitete sich der mysteriöse Wurm schnell in den Netzwerken der Opfer durch die gemeinsame Nutzung von USB-Geräten (Universal Serial Bus). Anfang Juni stieg die Zahl der Infektionen sprunghaft an, sodass Raspberry Robin Anfang August mit 17 % der von X-Force beobachteten Infektionsversuche seinen Höhepunkt erreichte. Dieser Spitzenwert wurde in der Öl- und Gasindustrie, in der Fertigungs- und der Transportbranche verzeichnet. Die Infektionsversuchsrate von 17 % in diesen Branchen ist signifikant, da insgesamt weniger als 1 % der Kunden von X-Force denselben Malware-Stamm feststellen konnten. Außerdem beobachtete X-Force von September bis November 2022 vermehrt Aktivitäten von Raspberry Robin.

Die Verbreitung von USB-basierten Würmern wird durch Social Engineering ermöglicht und erfordert für eine erfolgreiche Infizierung den physischen Zugriff auf ein Netzwerk oder einen Endpunkt, sei es durch einen berechtigten Benutzer oder auf andere Weise. X-Force empfiehlt sicherzustellen, dass Ihre Sicherheitstools bekannte USB-basierte Malware blockieren, Sicherheitsschulungen durchzuführen und Funktionen zur automatischen Ausführung für alle Wechseldatenträger zu deaktivieren. In besonders sensiblen Umgebungen wie der Betriebstechnologie oder in Bereichen mit Air Gaps ist es am sichersten, die Verwendung von USB-Laufwerken ganz zu verbieten. Zusätzlich zu den oben genannten Vorschlägen sollte die Anzahl der zugelassenen mobilen Geräte in Ihrer Umgebung streng kontrolliert werden.



Rust im Aufschwung

Die Programmiersprache Rust wurde 2022 bei Malware-Entwicklern immer beliebter, da sie plattformübergreifend unterstützt wird und die Erkennungsraten von Antivirenprogrammen im Vergleich zu anderen gängigeren Sprachen niedrig sind. Ähnlich wie bei der Programmiersprache Go ist das Kompilieren komplizierter, was die Analyse der Malware für das Reverse Engineering zeitaufwändiger machen kann. Mehrere Ransomware-Entwickler haben Rust-Versionen ihrer Malware veröffentlicht, darunter BlackCat, Hive, Zeon und vor Kurzem auch RansomExx. Darüber hinaus analysierte X-Force einen in Rust geschriebenen ITG23 Crypter sowie die CargoBay-Familie aus Backdoors und Downloadern. Die wachsende Popularität von Rust verdeutlicht, dass das Ransomware-Ökosystem weiterhin auf Innovationen setzt, um unerkannt zu bleiben.

InfoStealer Vidar

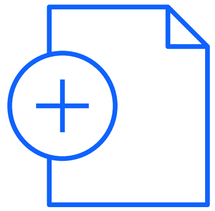
X-Force stellte einen plötzlichen Anstieg von Vidar InfoStealer Malware fest, der im Juni 2022 begann und bis Anfang 2023 anhielt. Vidar wurde erstmals 2018 beobachtet und ist ein böswilliger Trojaner, der als Info Stealer agiert und somit Informationen stiehlt. Er wird als Malware-as-a-Service (MaaS) verbreitet. Dieser Trojaner wird in der Regel ausgeführt, wenn Benutzer auf schädliche Spam Links (Malspam) oder -Anhänge klicken. Mithilfe seiner umfangreichen Funktionen kann Vidar eine Vielzahl von Gerätedaten wie Kreditkarteninformationen, Benutzernamen, Kennwörter und Dateien abrufen und Screenshots vom Desktop des Benutzers anfertigen. Vidar kann auch Bitcoin und Ethereum Wallets stehlen.

Angriffe durch einen Info Stealer sind in der Regel finanziell motiviert. Die gestohlenen Daten werden analysiert und alle wertvollen Informationen in einer Datenbank gesammelt und organisiert.

Diese Datenbank kann dann im Dark Web oder über die private Messaging-App Telegram verkauft werden. Für Kriminelle eröffnen sich mit diesen Informationen verschiedenste Betrugsmöglichkeiten, wie z. B. die Beantragung von Bankkrediten oder Kreditkarten, der Onlineeinkauf von Waren oder die Geltendmachung von Krankenversicherungsleistungen.

Bedrohungsakteure können kompromittierte Anmeldedaten verwenden, um auf Unternehmenskonten und Remotedienste zuzugreifen. Die durchschnittlichen Kosten für die Inanspruchnahme eines Info Stealers liegen bei etwa 250 USD pro Monat, wobei es den Benutzern überlassen bleibt, welche Malware sie einsetzen. X-Force stellt auf Marktplätzen immer wieder fest, dass dort durch Info-Stealer-Malware erbeutete Zugriffsberechtigungen für 10 bis 75 USD verkauft werden. Ist der Zugang erst einmal hergestellt, können Bedrohungsakteure die Berechtigungen des gehackten Kontos leicht als Ausgangspunkt für weitere böswillige Aktivitäten nutzen.

Entwicklung von Mechanismen zur Verbreitung von Malware



Immer häufiger wird Malware über schädliche Microsoft Office-Dokumente verbreitet, die meist an Phishing-E-Mails angehängt sind. Malware-Entwickler haben diese Dokumente mit schädlichen Makros erstellt, die beim Öffnen des Dokuments Malware ausführen. Die Verwendung von Makros zu diesem Zweck hat sich so weit verbreitet, dass Microsoft Office-Produkte Sicherheitswarnungen beim Öffnen von Dokumenten, bei denen Makros aktiviert sind, ausgeben. Seit Juli 2022 blockiert Microsoft standardmäßig die Ausführung von Makros in Dokumenten, die per E-Mail oder aus dem Internet empfangen werden.

Während die Sicherheitsexperten ihre Erkennungs- und Präventionsfähigkeiten verbesserten, begannen die Bedrohungsakteure, von Visual Basic Application (VBA) auf ein älteres Makroformat in Microsoft Excel umzusteigen, das als 4.0-Makro bekannt ist. Schädliche Excel-Dokumente werden schon seit langer Zeit eingesetzt. Die meisten Sicherheitsmechanismen wurden für VBA-Makros in Excel entwickelt. Eine Zeitlang eigneten sich Makros von Excel 4.0 perfekt dafür, unentdeckt zu bleiben. Etwa zur gleichen Zeit begannen einige Bedrohungsakteure damit, Links in E-Mails zu versenden, die das Opfer auf eine Dropper Webseite führten, damit sie von dort die schädlichen Dokumente herunterluden. Auf diese Weise mussten keine E-Mail-Anhänge mehr versendet werden. Als Microsoft Änderungen vornahm, sodass Administratoren 4.0-Makros deaktivieren und die Ausführung von aus dem Internet heruntergeladenen Makros blockieren konnten, waren die Bedrohungsakteure gezwungen, ihre Taktik erneut zu ändern.

Auch nach den von Microsoft vorgenommenen Änderungen verwenden viele Malware-Autoren immer noch Microsoft Office-Dokumente, bei denen Makros aktiviert sind. Fortschrittlichere Gruppen setzen jedoch eine kompliziertere und komplexere Infektionskette ein. Diese neuesten Taktiken umfassen eine Kombination aus HTML-Dateien, in die eine Binärdatei eingebettet ist, oder eine kennwortgeschützte komprimierte Datei. Diese Dateien enthalten auch ein ISO-Image, das eine LNK-Datei, eine CMD-Datei oder andere Dateitypen enthalten kann, bei denen es unwahrscheinlich ist, dass sie an einen E-Mail-Empfänger gesendet oder aus dem Internet heruntergeladen werden. Andere umfassen die Einschleusung von Vorlagen per Fernzugriff oder die Ausnutzung von Schwachstellen. CVE-2021-40444, eine Sicherheitslücke bei der Ausführung von Code per Fernzugriff in Microsoft HTML (MSHTML), ist ein Beispiel dafür, dass eine Softwarekomponente zum Rendern von Webseiten für die Ausführung von Malware in Microsoft Windows verwendet wird, ohne dass Makros zum Einsatz kommen.

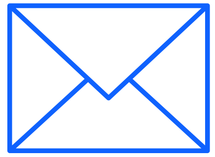
Spamdaten unterstreichen Ransomware-Bedrohung und verdeutlichen Makrotrends

X-Force analysierte Trends bei Phishing- und Spam-E-Mails, um ihre allgemeine Wirksamkeit und ihren Einsatz durch Bedrohungsakteure besser verstehen zu können. Die Untersuchung ergab, dass Spam-E-Mails das ganze Jahr über regelmäßig zur Verbreitung von Malware wie Emotet, Qakbot, IcedID und Bumblebee eingesetzt wurden, was häufig Ransomware-Infektionen zur Folge hatte.

Malware[10–18]	**Ransomware**
Trickbot	*Conti*
Bazarloader	*Conti*, Diavol
IcedID	*Conti*, Quantum
Bumblebee	*Conti*, Diavol, Quantum
Emotet	*Conti*, BlackCat, Quantum
Qakbot	*REvil*, *Conti*, Black Basta
SocGholish	LockBit

Die Daten in dieser Tabelle beziehen sich auf den Zeitraum von Ende 2021 bis zur Veröffentlichung dieses Berichts. Kursivschrift bedeutet, dass die Malware oder Ransomware 2022 entdeckt, aber bis mindestens Oktober 2022 nicht von X-Force beobachtet wurde.

X-Force stellte im September 2022 eine Häufung von Qakbot-Aktivitäten fest, bei denen HTML-Malware zur Kompromittierung von Infektionszielen eingesetzt wurde. Diese Infektionen sind mit umfangreichen Aktivitäten nach der Kompromittierung verbunden, einschließlich Ausspähung, Informationsbeschaffung und Bereitstellung zusätzlicher Schadteile. Unkontrollierte Qakbot-Infektionen führten 2022 zu zahlreichen Black-Basta-Infektionen. X-Force stellte fest, dass Ransomware-Attacken, die auf der Leak Site der Ransomware-Gruppe Black Basta gemeldet wurden, während der Unterbrechung der Phishing-Aktivitäten von Qakbot im Sommer 2022 deutlich zurückgingen. X-Force geht davon aus, dass die Wiederaufnahme der Qakbot-Aktivitäten in ähnlicher Weise mit einem Anstieg der Ransomware-Opfer korrelieren wird.



Umgehung von Makros

Als Reaktion auf die Makroänderungen von Microsoft ab Oktober 2021 hat sich die Verwendung von ISO- und LNK-Dateien zu einer wichtigen Taktik für die Infizierung von Unternehmen entwickelt. Diese Taktik beinhaltet die direkte Bereitstellung von Schadteilen über solche Containerdateien. Dies umfasst auch die Verschleierung von mit Makros aktivierten Dateien.

- Mit ISO-Dateien und komprimierten Dateien kann das von Microsoft verwendete MOTW-Attribut (Mark of the Web) umgangen werden. Somit werden die Ziele dafür genutzt, schädliche Makros zu aktivieren. Während die ISO- oder komprimierten Dateien so aussehen, als seien sie aus dem Internet heruntergeladen worden, ist dies bei dem mit Makros aktivierten Anhang nicht der Fall, was dazu führt, dass Bedrohungsakteure den Angriff fortsetzen können.
- Makrobeschränkungen können auch dadurch umgangen werden, dass Schadteile direkt in LNK-Dateien eingebettet werden, die beim Anklicken willkürliche Befehle auslösen, die üblicherweise zum Herunterladen oder Laden der nächsten Schritte verwendet werden. Bis Anfang 2022 gab es nur eine Kampagne im Februar 2021, bei der diese Taktik zum Einsatz kam. X-Force beobachtete dies erstmalig Ende Februar/März 2022 und aktuell wieder regelmäßig.

Weitere Trends, die X-Force bei den Spamkampagnen der Bedrohungsakteure festgestellt hat, sind die zunehmende Verwendung verschlüsselter, komprimierter Archive als Anhänge und Thread Hijacking, wie hier beschrieben.

- Verschlüsselte komprimierte Erweiterungen, die für Antivirensoftware schwerer zu erkennen und als schädlich einzustufen sind, wurden 2022 häufiger entdeckt. Die durchschnittliche Anzahl der pro Woche zugestellten Spam-E-Mails, die solche Anhänge enthalten, hat sich 2022 verglichen mit den Daten für 2021 seit April desselben Jahres verneunfacht.
- Thread Hijacking, bei dem sich Bedrohungsakteure in bestehende E-Mail-Threads einklinken, ist eine seit Langem angewandte Taktik, um die Legitimität von Spam zu erhöhen und Opfer effektiver zum Handeln zu bewegen. Diese Taktik nahm 2022 – im Vergleich zum Großteil des Jahres 2021 – deutlich zu und flachte im Frühjahr wieder ab, ein Trend, der laut X-Force größtenteils auf Emotet-Spamming zurückzuführen ist.

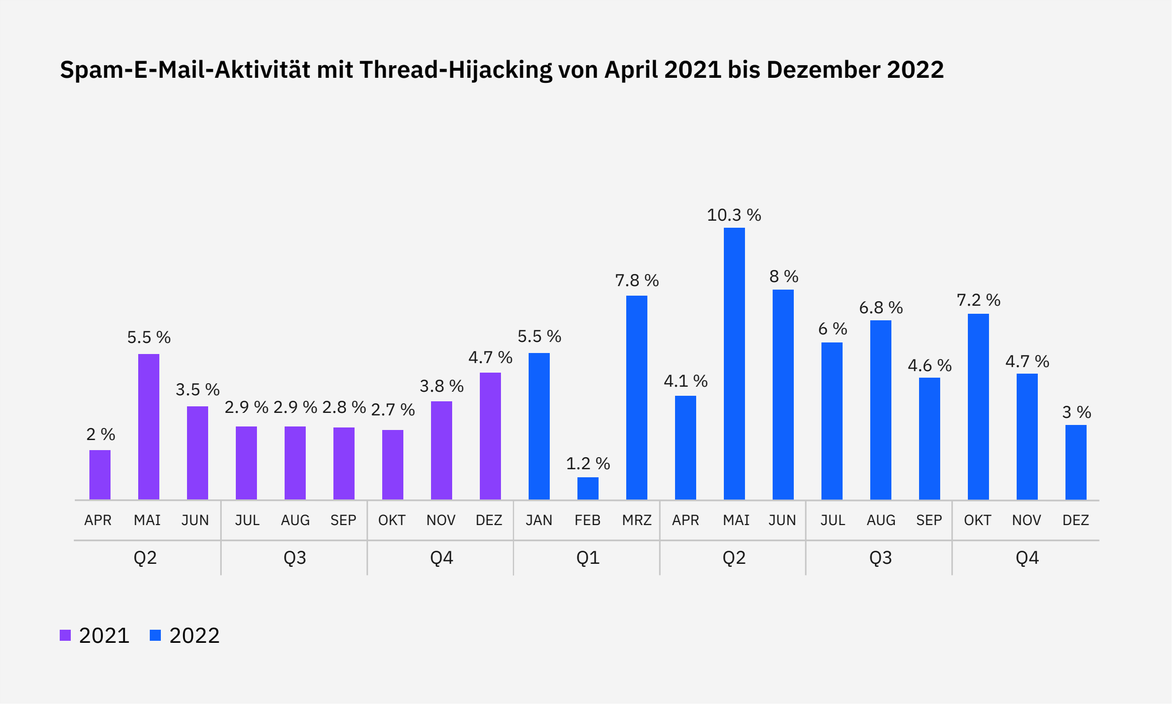


Abbildung 13: Die Zahlen zeigen den prozentualen Anteil aller Thread-Hijacking-Versuche, die seit April 2021 in den X-Force-Daten entdeckt wurden, aufgeschlüsselt nach Monaten. Quelle: X-Force

– Emotet kehrte im November 2021 zurück, nachdem das Botnet im Januar 2021 zerschlagen worden war. Die Malware war bis 2022 aktiv, pausierte ab Mitte Juli fast vier Monate lang und kehrte im November 2022 für circa zwei Wochen zurück.

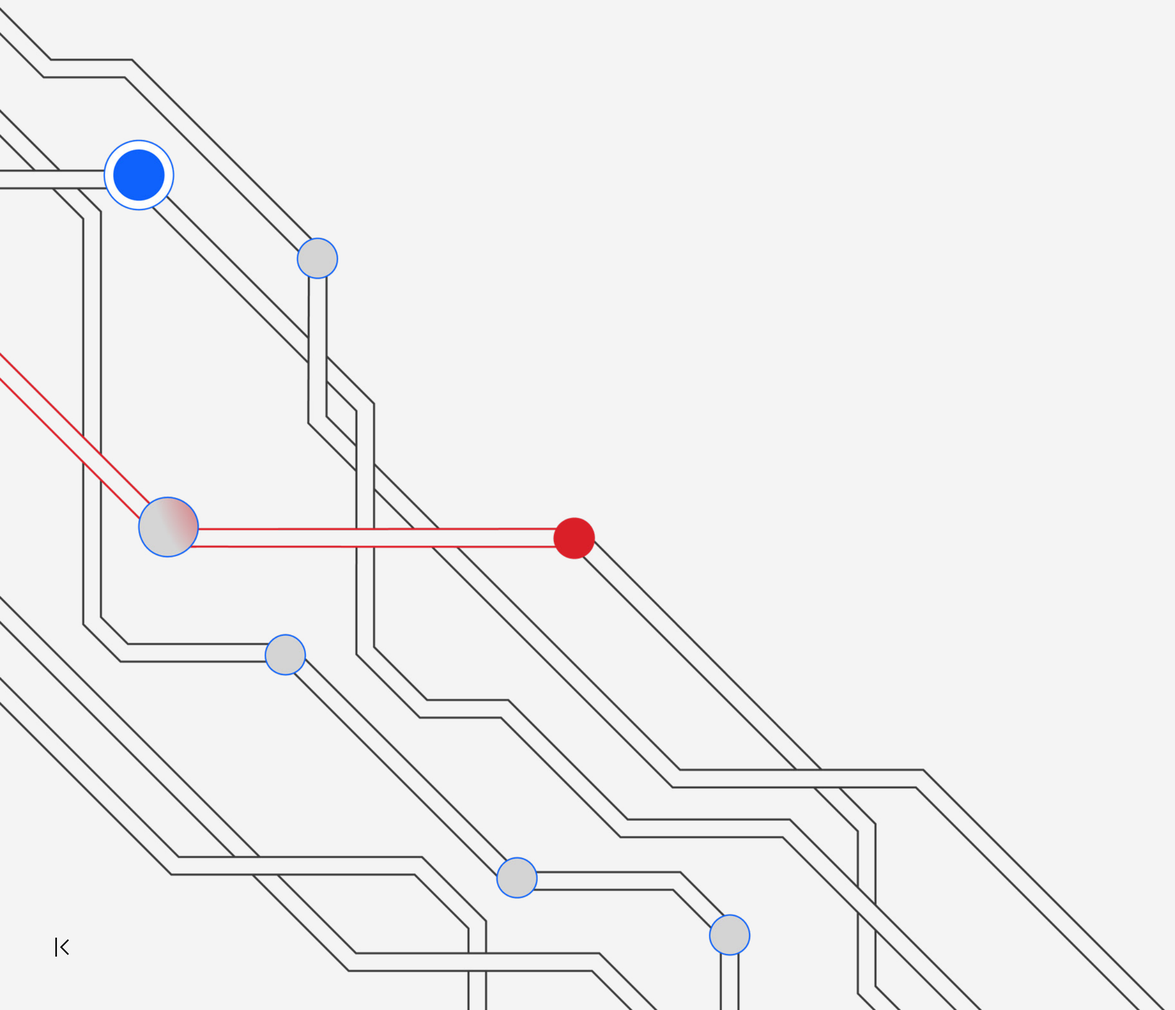
– Die Daten zeigen, dass im Jahr 2022 etwa doppelt so viele reguläre Versuche pro Monat durchgeführt wurden wie seit April 2021. Thread Hijacking fand bis Mai 2022 eher unregelmäßig statt und der Rückgang in der zweiten Jahreshälfte entspricht in etwa der Inaktivität von Emotet.

– Thread-Hijacking wurde häufig in Verbindung mit Spam-E-Mails verwendet, die auf Emotet, Qakbot und IcedID zurückzuführen waren. Die Rückkehr von Emotet im November 2021 trug zum unsteten Anstieg bis Mai 2022 bei. Der allgemeine Rückgang in der zweiten Jahreshälfte lässt sich mit der Pause von Emotet von Juli bis Oktober und der kurzen Rückkehr im November 2022 erklären.

– Thread Hijacking lässt sich schwer nachverfolgen und ebenso schwer von Vorfällen abgrenzen, in denen böswillige Akteure einfach eine Antwort-Betreffzeile an eine Spam-E-Mail anhängen. Es ist davon auszugehen, dass dies in Zukunft noch schwieriger werden wird. So haben beispielsweise einige Bedrohungsakteure damit begonnen, die Betreffzeile „Re:“ zu entfernen, wahrscheinlich, weil sie mittlerweile wissen, dass diese Angabe zur Verfolgung ihrer Aktivitäten verwendet werden kann.

09

Bedrohungen für OT und industrielle Steuersysteme



Bedrohungen für die Betriebstechnik

Im Jahr 2022 wurden zwei neue OT-spezifische Schadprogramme entdeckt: Industroyer2 und INCONTROLLER, auch PIPEDREAM genannt, sowie zahlreiche OT-Schwachstellen, bekannt als OT:ICEFALL. Die Cyberbedrohungslandschaft für OT weitet sich dramatisch aus, und die Betreiber und Bediener von OT-Anlagen müssen sich der ständig ändernden Landschaft bewusst sein.

X-Force hat OT-spezifische Netzattacken und IR-Daten genauer untersucht, um Erkenntnisse darüber zu gewinnen, wie Bedrohungsakteure versuchen, Kunden in OT-bezogenen Branchen zu kompromittieren. Daten über Netzattacken zeigen, dass Brute-Force-Attacken, die Verwendung schwacher und veralteter Verschlüsselungsstandards sowie schwache oder Standardkennwörter in den IT- und OT-Umgebungen dieser Branchen weitverbreitet sind.

Alerts, die auf wahrscheinliche Versuche von Brute-Force-Attacken hinweisen, wurden bei den ICS-spezifischen Daten der Netzattacken am häufigsten beobachtet, dicht gefolgt von Alerts zu schwacher Verschlüsselung. Die häufigsten Alerts aufgrund schwacher Verschlüsselung betrafen die anhaltende Verwendung von Transport Layer Security (TLS) 1.0, einer seit März 2021 nicht weiterentwickelten, veralteten und unsicheren Verschlüsselungsmethode. Obwohl die US-Regierung eine Migration zu TLS 1.2 oder 1.3 empfiehlt, befassen sich die Richtlinien des National Institute of Standards and Technology (NIST) umfassender mit den realen Umständen. Denn in der Realität müssen ältere Systeme möglicherweise weiterhin schwächere Verschlüsselungsversionen zur Gewährleistung ihrer Funktionalität verwenden. Bemerkenswert waren auch die Alerts zu schwachen oder Standardkennwörtern, zumal es sich hierbei um grundlegende

Schwachstellen handelt, die Brute-Force-Attacken für Angreifer einfacher machen. Das weitverbreitete und wahrscheinlich wahllose Scannen nach internen und externen Sicherheitslücken stellte den häufigsten Angriffsversuch gegen OT-bezogene Branchen dar. Die Daten zeigen, dass alte Schwachstellen und Bedrohungen auch heute noch aktuell sind. Eine Gruppe von Sicherheitslücken, die 2021 von Cisco Talos in der Überwachungssoftware Advantech R-SeeNet entdeckt wurde, löste 2022 eine knappe Mehrheit der Alerts beim Scannen nach Schwachstellen in allen OT-Branchen aus. Diese Sicherheitslücken könnten Angreifern das Ausführen von beliebigem Code oder willkürlichen Befehlen ermöglichen.

Die zweithäufigste Schwachstelle stammt jedoch von 2016 – es handelt sich hierbei um eine Sicherheitslücke zur Filterumgehung in der Anwendung Trihedral VTScada (CVE-2016-4510), die es nicht authentifizierten Benutzern ermöglichen könnte, HTTP-Anfragen für Dateizugriffe zu senden. Ein weiterer Hinweis auf die Risiken älterer Bedrohungen sind Angriffstypen wie WannaCry und Conficker, die nach wie vor eine erhebliche Bedrohung für die Betriebstechnik darstellen.

Fertigung nach wie vor die am stärksten betroffene OT-Branche

Betrachtet man die Untergruppe der Vorfälle in OT-bezogenen Branchen, so wurde den Daten zufolge die Fertigung 2022 am häufigsten angegriffen. Diese Branche wurde in 58 % der Fälle geschädigt, bei denen X-Force zur Lösung beitrug. Die Verwendung von Backdoors war hierbei die am weitesten verbreitete Maßnahme, die in 28 % der Fälle in der Fertigungsbranche beobachtet wurde. Insbesondere Ransomware-Akteure finden in dieser Branche ein attraktives Ziel, vermutlich, weil diese Unternehmen nur über eine geringe Toleranz gegenüber Ausfallzeiten verfügen.

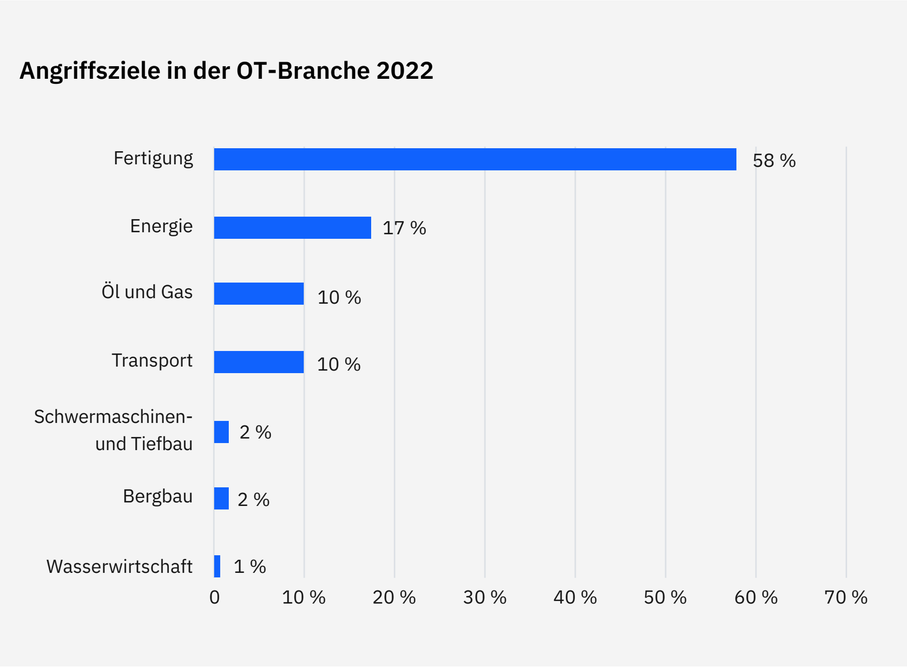


Abbildung 14: Anteil der IR-Vorfälle nach OT-bezogenen Branchen, auf die X-Force 2022 reagiert hat.
Quelle: X-Force

Betrachtet man die ursprünglichen Zugriffsvektoren bei Fällen in OT-bezogenen Branchen, so wurde in 38 % der Fälle Spear-Phishing eingesetzt, davon in 22 % über Anhänge, in 14 % über Links und in 2 % über Spear-Phishing-as-a-Service. Die Nutzung von Anwendungen mit Internet-Schnittstelle lag mit 24 % an zweiter Stelle und folgte damit dem allgemeinen Trend der Branche. Auch die Erkennung von Backdoors war mit 20 % der Vorfälle in diesen Branchen führend, gefolgt von Ransomware mit 19 %. Erpressung bleibt mit 29 % ebenfalls an erster Stelle der Auswirkungen, dicht gefolgt von Datendiebstahl mit 24 % der Vorfälle.

Das Fehlen einer angemessenen Segmentierung zwischen OT- und IT-Netzwerken birgt eine weitere große Schwachstelle, die in der Betriebstechnik ausgenutzt wird. Das Team von X-Force Red Adversary Simulation Services zielt regelmäßig auf eine schwache Segmentierung ab, um Zugang zu isolierten OT-Umgebungen zu erhalten. Zu diesen Umgebungen gehören Targeting Jump Server, dual-homed Bedienerarbeitsplätze und Berichtsserver, wie z. B. Data Historians, die Web- und SQL-Services der OT in unternehmensweiten IT-Netzwerken freigeben. Die richtige Segmentierung dieser Teile Ihrer Netzwerke und die genaue Beobachtung der Kommunikation zwischen ihnen kann die Sicherheit Ihrer Assets gewährleisten.

Geografische Trends

Das zweite Jahr in Folge steht der asiatisch-pazifische Raum an der Spitze der 2022 am häufigsten angegriffenen Regionen. 31 % der Vorfälle, auf die X-Force IR reagierte, entfielen auf diese Region. Europa folgte mit 28 % der Angriffe und Nordamerika mit 25 % der Vorfälle. Im asiatisch-pazifischen Raum und in Europa stieg der Anteil gegenüber 2021 um fünf bzw. vier Prozentpunkte, während im Nahen Osten ein deutlicher Rückgang von 14 % auf 4 % zu verzeichnen ist.

Vorfälle nach Region 2020–2022

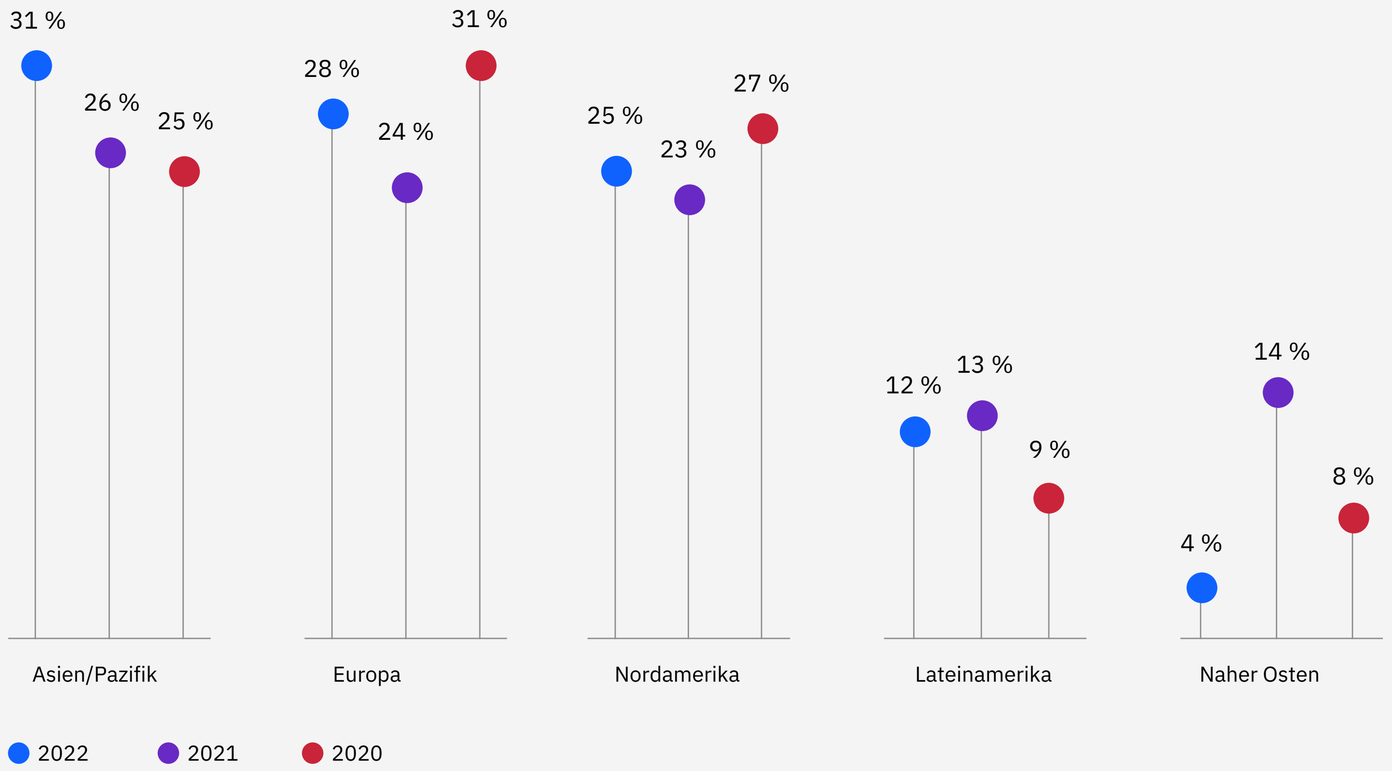


Abbildung 15: Anteil der IR-Vorfälle nach Region, auf die X-Force von 2020 bis 2022 reagiert hat. Quelle: X-Force

Nr. 1 | Asiatisch-pazifischer Raum

Der asiatisch-pazifische Raum, insbesondere Japan, bildete das Zentrum des Emotet-Spitzenwerts 2022. Der Anstieg der Emotet-Fälle in Japan stand zwar nicht in direktem Zusammenhang mit dem Krieg in Europa, fiel aber zeitlich mit der russischen Invasion in der Ukraine zusammen, die laut anderen Forschern aus der Cybersicherheit-Community zu einem erheblichen Anstieg der Emotet-Aktivitäten in diesem Zeitraum beitrug. Spamkampagnen wurden in verschiedenen Branchen beobachtet, wobei die meisten Fälle in der Fertigung sowie im Finanz- und Versicherungssektor auftraten. Emotet wird hauptsächlich durch Spamkampagnen mit aufmerksamkeitserregendem Titel verbreitet.

Die Fertigungsbranche führt die Liste der angegriffenen Branchen in dieser Region mit 48 % der Vorfälle an, während der Finanz- und Versicherungssektor mit 18 % weit abgeschlagen an zweiter Stelle liegt.

Spear-Phishing durch Anhänge galt mit 40 % als der wichtigste Infektionsvektor in dieser Region, gefolgt von der Ausnutzung von Anwendungen mit Internet-Schnittstelle mit 22 %. Vorfälle mit externen Services per Fernzugriff und Spear-Phishing-Links liegen mit 12 % an dritter Stelle.

Die Einrichtung von Backdoors war mit 31 % der Fälle in der Region die häufigste Angriffsmethode. An zweiter Stelle steht Ransomware mit 13 % und an dritter Stelle Maldocs mit 10 %. Erpressung war die häufigste Auswirkung, die in 28 % der Fälle beobachtet wurde. An zweiter Stelle steht die Schädigung des Markenrufs mit 22 % und an dritter Stelle der Datendiebstahl mit 19 %.

Auf Japan entfielen 91 % der Fälle im asiatisch-pazifischen Raum, auf die Philippinen 5 % und auf Australien, Indien und Vietnam jeweils 1,5 %.

Der am häufigsten angegriffene Wirtschaftszweig im asiatisch-pazifischen Raum betraf die Fertigungsbranche mit einem Anteil von 48 %.

Nr. 2 | Europa

In Europa konnte ab März 2022, kurz nach der Invasion der Ukraine durch Russland, ein deutlicher Anstieg der Backdoor-Bereitstellungen verzeichnet werden. Der Einsatz von Backdoors machte 21 % der Vorfälle in der Region aus, Ransomware 11 %. Bei 10 % der Vorfälle, auf die X-Force reagierte, wurden Fernzugriffstools identifiziert. Bei den Auswirkungen auf Kunden standen 38 % der von X-Force in Europa beobachteten Vorfälle mit Erpressung in Verbindung, 17 % führten zu Datendiebstahl und 14 % zum Ausspähen von Anmeldedaten. Europa stellte mit 44 % aller beobachteten Erpressungsfälle die am stärksten betroffene Region dar.

Die Ausnutzung von Anwendungen mit Internet-Schnittstelle galt mit 32 % aller von X-Force in der Region bearbeiteten Vorfälle als wichtigster Infektionsvektor für europäische Unternehmen, wobei mehrere davon zu Infektionen mit Ransomware führten. An zweiter Stelle stand der Missbrauch gültiger lokaler Konten mit 18 %, gefolgt von Spear-Phishing-Links mit 14 %, was einen deutlichen Rückgang gegenüber 42 % im Jahr 2021 darstellt. Dieser Rückgang von Spear-Phishing-Links kann auf eine bessere Sensibilisierung der Nutzer, eine verbesserte E-Mail-Sicherheit oder eine wirksamere Abwehr von Malware nach der Installation zurückzuführen sein.

Professional-, Geschäfts- und Verbraucherservices waren zusammen mit Finanz- und Versicherungsservices die am häufigsten angegriffenen Branchen (jeweils 25 % der Fälle, auf die X-Force reagierte). An zweiter Stelle folgt die Fertigungsbranche mit 12 % der Vorfälle, und an dritter Stelle liegen Energie und Gesundheitswesen mit 10 %.

Das Vereinigte Königreich war mit 43 % der Fälle das am stärksten betroffene Land in Europa. Auf Deutschland entfielen 14 %, auf Portugal 9 %, auf Italien 8 % und auf Frankreich 7 %. Auch in Norwegen, Dänemark, der Schweiz, Österreich, Griechenland, Grönland, Spanien und Serbien ist die Zahl der Vorfälle zurückgegangen.

Das Vereinigte Königreich galt mit 43 % der Fälle als das am stärksten betroffene Land in Europa.

Nr. 3 | Nordamerika

X-Force beobachtete einen leichten Anstieg der Vorfälle in Nordamerika von 23 % aller Fälle 2021 auf 25 % im Jahr 2022.

Energieunternehmen standen an der Spitze der Liste Betroffener in Nordamerika und stellten 20 % aller Angriffe dar, auf die X-Force 2022 reagierte. An zweiter Stelle folgten die Fertigung und der Einzel- und Großhandel mit jeweils 14 %. Während der Einzel- und Großhandel 2021 eine ähnliche Position einnahm, hat sich der Anteil der Fertigungsbranche gegenüber 2021 halbiert. Professional-, Geschäfts- und Verbraucherservices standen 2022 mit 12 % an dritter Stelle, da die Zahl der Fälle von Ransomware und anderer Schadsoftware zunimmt.

Die am häufigsten identifizierten Infektionsvektoren waren die Ausnutzung von Anwendungen mit Internet-Schnittstelle (35 %) und Spear-Phishing-Anhänge (20 %).

Ransomware-Vorfälle machten 23 % der Fälle aus, von denen einige auf die Erkennung anhaltender Infektionen mit WannaCry oder Ryuk in den Jahren 2018 oder 2019 zurückzuführen waren, was die Bedeutung einer ordnungsgemäßen Bereinigung nach solchen Ereignissen unterstreicht. In der Region waren 12 % der Fälle auf Botnets zurückzuführen, gefolgt von Backdoors und BECs mit jeweils 10 %.

Bei der Betrachtung der wichtigsten Auswirkungen von Bedrohungsakteuren steht das Ausspähen von Anmeldedaten mit 25 % der von X-Force in Nordamerika bearbeiteten Vorfälle an erster Stelle. Datenlecks und Datendiebstahl standen mit jeweils 17 % an zweiter Stelle, während Erpressung 13 % der Fälle ausmachte.

Auf die Vereinigten Staaten entfielen 80 % der Angriffe in der Region, auf Kanada dagegen nur 20 %.

Die am häufigsten angegriffenen Unternehmen in Nordamerika betrafen mit 20 % der Fälle Energieunternehmen.

Nr. 4 | Lateinamerika

Zum Zweck der Berichterstellung betrachtet IBM Mexiko, Zentralamerika und Südamerika als zu Lateinamerika gehörend.

Die Vorfälle in Lateinamerika entwickelten sich entgegen dem weltweiten Trend, sodass der Einzelhandel mit 28 % der von X-Force bearbeiteten Fälle erneut die am häufigsten angegriffene Branche darstellt. Im Jahr 2021 lag dieser Sektor noch an zweiter Stelle. Der Finanz- und Versicherungssektor war mit 24 % der Fälle am zweithäufigsten betroffen, gefolgt vom Energiesektor mit 20 %.

Ransomware-Attacken übertrafen andere Angriffe in Lateinamerika und machten 32 % der Fälle aus, auf die X-Force reagierte. Die Verwendung von Backdoors verzeichnete mit 16 % die am zweithäufigsten identifizierte Angriffsmethode, während BEC und E-Mail Thread Hijacking mit jeweils 11 % an dritter Stelle lagen. Erpressung und Datendiebstahl waren mit 27 % der Fälle die am häufigsten beobachteten Auswirkungen in der Region, während die finanziellen Verluste 20 % betrugen. An dritter Stelle folgen Datenvernichtung und Datenlecks mit jeweils 13 % der Fälle.

Die wichtigsten ursprünglichen Zugriffsvektoren bildeten externe Remote-Services mit 30 % und die Ausnutzung öffentlich verfügbarer Anwendungen mit 20 %. Jeweils 10 % entfielen auf Drive-by-Kompromittierungen, Hardwareerweiterungen, Domänenkonten, gültige lokale Konten und Spear-Phishing-Anhänge.

Von allen Fällen, die von X-Force in Lateinamerika bearbeitet wurden, entfielen 67 % auf Brasilien, 17 % auf Kolumbien und 8 % auf Mexiko. Peru und Chile teilten sich die verbleibenden 8 %.

In Lateinamerika entfielen 67 % der von X-Force bearbeiteten Fälle auf Brasilien.

Nr. 5 | Naher Osten und Afrika

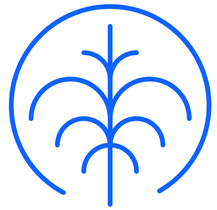
Zum Zweck der Berichterstellung betrachtet IBM die Levante, die Arabische Halbinsel, Ägypten, Iran und Irak sowie den gesamten afrikanische Kontinent zur Region Naher Osten und Afrika gehörend.

In 27 % der Fälle, auf die X-Force im Jahr 2022 in dieser Region reagierte, wurden Backdoor-Bereitstellungen festgestellt. Ransomware und Würmer galten mit jeweils 18 % als zweithäufigste Angriffsart. Erpressung und finanzieller Schaden machten 2021 jeweils die Hälfte der festgestellten Auswirkungen der Vorfälle in der Region aus.

In zwei Dritteln der Fälle wurden Spear-Phishing-Links für den Erstzugriff verwendet, das andere Drittel der von X-Force im Nahen Osten und Afrika bearbeiteten Vorfälle betraf Wechseldatenträger. Der Finanz- und Versicherungssektor war 2022 mit 44 % der Vorfälle die am häufigsten angegriffene Branche im Nahen Osten und Afrika, ein leichter Rückgang gegenüber 2021 mit 48 %. Auf den Bereich der Professional-, Geschäfts- und Verbraucherservices entfielen 22 % der Angriffe, an dritter Stelle folgten die Fertigungsbranche und der Energiesektor mit 11 %.

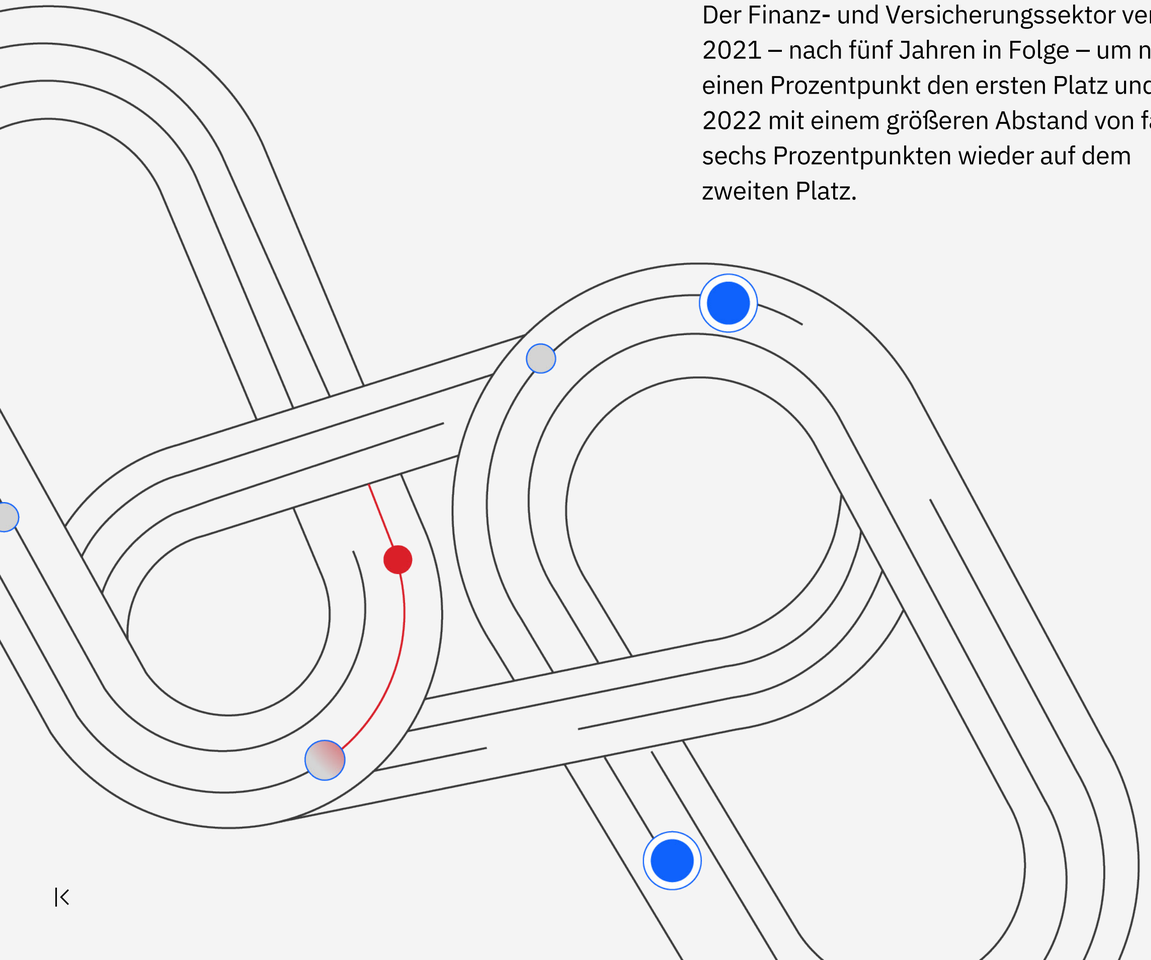
In Saudi-Arabien ereigneten sich zwei Drittel der Fälle in der Region, auf die X-Force reagierte. Die übrigen Fälle verteilten sich auf Katar, die Vereinigten Arabischen Emirate und Südafrika.

Die häufigste Angriffsart in dieser Region erfolgte mit 27 % der Fälle durch die Bereitstellung von Backdoors.



Branchentrends

Das zweite Jahr in Folge war die Fertigung die am häufigsten angegriffene Branche, wie X-Force IR-Daten zeigen. Der Finanz- und Versicherungssektor verliert 2021 – nach fünf Jahren in Folge – um nur einen Prozentpunkt den ersten Platz und liegt 2022 mit einem größeren Abstand von fast sechs Prozentpunkten wieder auf dem zweiten Platz.



Anteil der Angriffe nach Branchen 2018–2022

Branche	2022	2021	2020	2019	2018
Fertigung	24,8 %	23,2	17,7	8	10
Finanzen und Versicherungen	18,9 %	22,4	23	17	19
Professional-, Geschäfts- und Verbraucherservices	14,6 %	12,7	8,7	10	12
Energie	10,7 %	8,2	11,1	6	6
Einzel- und Großhandel	8,7 %	7,3	10,2	16	11
Bildung	7,3 %	2,8	4	8	6
Gesundheitswesen	5,8 %	5,1	6,6	3	6
Öffentliche Verwaltung	4,8 %	2,8	7,9	8	8
Transport	3,9 %	4	5,1	13	13
Medien und Telekommunikation	0,5 %	2,5	5,7	10	8

24,8 %

der von X-Force bearbeiteten Vorfälle betrafen den Fertigungssektor.

Nr. 1 | Fertigung

Die Fertigungsbranche war mit einem etwas größeren Abstand zum Nächstplatzierten als noch 2021 der am stärksten betroffene Wirtschaftsbereich. Im Jahr 2022 wurden Backdoors bei 28 % der Vorfälle eingesetzt und übertrafen damit Ransomware, die bei 23 % der von X-Force bearbeiteten Vorfälle zum Einsatz kam. Der prozentuale Anteil der Backdoor-Bereitstellungen ist ebenfalls auf die erhöhten Infektionen mit Emotet-Viren zurückzuführen. Einige dieser Fälle hätten zu Ransomware-Attacken und anderen böswilligen Aktivitäten führen können, konnten jedoch früh genug erkannt und behoben werden.

Spear-Phishing-Anhänge und die Ausnutzung von Anwendungen mit Internet-Schnittstelle ergaben mit jeweils 28 % die beiden wichtigsten Infektionsvektoren. Externe Services per Fernzugriff standen mit 14 % an zweiter Stelle, während sich Spear-Phishing-Links und gültige Standardkonten für den Erstzugriff mit jeweils 10 % der Fälle den dritten Platz teilten.

Erpressung war in 32 % der Fälle die wichtigste Auswirkung auf Fertigungsunternehmen. Es ist bekannt, dass Hersteller wenig oder keine Toleranz für Ausfallzeiten haben. Genau diese Intoleranz macht Erpressung zu einer lukrativen Strategie für Angreifer. Auf Datendiebstahl entfiel mit 19 % der Vorfälle die zweithäufigste Auswirkung, gefolgt von Datenlecks mit 16 %. Im asiatisch-pazifischen Raum ereigneten sich mit rund 61 % die meisten Vorfälle in der Fertigungsbranche. Europa und Nordamerika folgten mit 14 %, Lateinamerika mit 8 % und der Nahe Osten und Afrika mit 4 %.

18,9 %

der von X-Force bearbeiteten Vorfälle betrafen den Finanz- und Versicherungssektor.

Nr. 2 | Finanzen und Versicherung

Auf Finanz- und Versicherungsunternehmen entfielen 2022 weniger als einer von fünf Angriffen, auf die X-Force reagierte. Dieser Anteil weist einen leichten Rückgang innerhalb der letzten Jahre auf, da andere Branchen, insbesondere die Fertigung, in den Fokus der Angreifer gerückt sind.

Finanz- und Versicherungsunternehmen sind in der Regel sowohl bei der digitalen Transformation als auch bei der Einführung von Cloud Computing weiter fortgeschritten als andere Branchen. Die Folge ist, dass Angreifer für erfolgreiche Angriffe auf diese Unternehmen unter Umständen einen Mehraufwand betreiben müssen.

Angriffe über Backdoors waren mit 29 % die am häufigsten beobachteten Angriffsmethoden, gefolgt von Ransomware und Maldocs mit jeweils 11 %. Den häufigsten Infektionsvektor stellten Spear-Phishing-Anhänge dar, die bei 53 % der Angriffe in diesem Sektor verwendet wurden. Die Ausnutzung von Anwendungen mit Internet-Schnittstelle stand mit 18 % der Angriffe an zweiter Stelle, und Spear-Phishing-Links bildeten in 12 % der Fälle den ursprünglichen Zugriffsvektor.

Die meisten Angriffe auf Finanz- und Versicherungsunternehmen fanden in Europa statt (ca. 33 % aller Angriffe), während der asiatisch-pazifische Raum mit ca. 31 % knapp dahinter liegt. Auf Lateinamerika entfielen etwa 15 % der Vorfälle, auf die X-Force reagierte, auf Nordamerika sowie den Nahen Osten und Afrika jeweils rund 10 %.

14,6 %

der von X-Force bearbeiteten Vorfälle betrafen Professional-, Geschäfts- und Verbraucherservices.

Nr. 3 | Professional-, Geschäfts- und Verbraucherservices

Die Branche für Professional Services umfasst Beratungsunternehmen, Verwaltungsgesellschaften und Anwaltskanzleien. 52 % der Betroffenen in diesem Segment gehören zu dieser Dienstleistungsbranche. Zu den Geschäftsservices zählen dagegen Firmen wie IT- und Technologiedienstleister, Öffentlichkeitsarbeit, Werbung und Kommunikation. 37 % aller Betroffenen gehören zu diesem Bereich. Verbraucherservices, einschließlich Bauwesen, Immobilien, Kunst, Unterhaltung und Erholung, machten 11 % der Fälle aus. Zusammen bilden sie die Kategorie „Professional-, Geschäfts- und Verbraucherservices“ des X-Force Threat Intelligence Index 2023.

Am häufigsten betroffen von Ransomware-Attacken und Angriffen über Backdoors waren mit jeweils 18 % der Fälle Geschäfts- und Verbraucherservices. Die wichtigsten identifizierten Infektionsvektoren machten die Ausnutzung von Anwendungen mit Internet-Schnittstelle und externe Services per Fernzugriff mit jeweils 23 % aus. Spear-Phishing-Anhänge und gültige lokale Konten galten in jeweils 15 % der Fälle als Ursache.

Erpressung war in 28 % der Fälle die häufigste Auswirkung, während Datendiebstahl, Ausspähen von Anmeldedaten und Datenlecks jeweils 17 % ausmachten. X-Force reagierte auf 47 % der Fälle in Europa, 33 % in Nordamerika, 10 % im asiatisch-pazifischen Raum, 7 % im Nahen Osten und Afrika und 3 % in Lateinamerika.

10,7 %

der von X-Force bearbeiteten Vorfälle betrafen den Energiesektor.

Nr. 4 | Energie

Energieunternehmen, darunter Stromversorger sowie Öl- und Gasunternehmen, stellten mit 10,7 % der Angriffe wie 2021 die am vierthäufigsten angegriffene Branche dar. Die Ausnutzung von Anwendungen mit Internet-Schnittstelle war hierbei mit 40 % der häufigste Infektionsvektor. Auf Spear-Phishing-Links und externe Services per Remote-Zugriff entfielen jeweils 20 % der Fälle. Botnets machten in 19 % der Fälle die häufigste Angriffsmethode aus, während Ransomware und BEC mit 15 % an zweiter Stelle standen.

Datendiebstahl und Erpressung wurden in 23 % der Fälle festgestellt, gefolgt vom Ausspähen von Anmeldedaten und Botnet-Infektionen mit jeweils 15 %. Aus allen von X-Force weltweit bearbeiteten Fällen waren nordamerikanische Unternehmen mit 46 % am häufigsten betroffen, gefolgt von Europa und Lateinamerika mit jeweils 23 % und dem asiatisch-pazifischen Raum sowie dem Nahen Osten und Afrika mit knapp 5 %.

Der Energiesektor steht nach wie vor unter dem Druck verschiedener globaler Kräfte, insbesondere derer, die durch den Krieg Russlands in der Ukraine und dessen Auswirkungen auf den ohnehin turbulenten Weltenergiehandel noch verstärkt wurden.

8,7 %

der von X-Force bearbeiteten Vorfälle betrafen den Einzel- und Großhandelssektor.

Nr. 5 | Einzel- und Großhandel

Einzelhändler sind für den Verkauf von Waren an Verbraucher und Großhändler zuständig. Großhändler sind in der Regel für den Transport und die Verteilung dieser Waren direkt von den Herstellern an die Einzelhändler oder direkt an die Verbraucher zuständig. Der Einzel- und Großhandel war laut IR-Daten von X-Force die am fünfthäufigsten betroffene Branche, genau wie im Ranking von 2021.

Der häufigste ursprüngliche Zugriffsvektor bei Angriffen auf den Einzel- und Großhandel bildeten Spear-Phishing-E-Mails mit einem schädlichen Link (33 %). Jeweils 17 % entfielen auf kompromittierte externe Services per Fernzugriff, Spear-Phishing mit schädlichen Anhängen und Hardwareerweiterungen.

Ransomware, Backdoors und BECs machten mit jeweils 19 % die am häufigsten eingesetzten Aktivitäten der Angreifer aus. Würmer wurden in 10 % der Fälle entdeckt. In 50 % der Fälle wurden die Opfer erpresst, in jeweils 25 % der Fälle kam es zum Ausspähen von Anmeldedaten und zu finanziellem Verlust. Die meisten Fälle ereigneten sich in Nord- und Lateinamerika mit jeweils 39 %. In Europa waren es nur 22 %.

7,3 %

der von X-Force bearbeiteten Vorfälle betrafen den Bildungssektor.

Nr. 6 | Bildung

20 % der Angriffe im Bildungsbereich, auf die X-Force reagiert hat, beinhalteten Backdoors. Ransomware, Adware und Spam machten jeweils 13 % aus. Die Ausnutzung von Anwendungen mit Internet-Schnittstelle war in 42 % der Fälle der häufigste beobachtete Erstzugriff, gefolgt von Spear-Phishing-Anhängen mit 25 %. Phishing über einen Service, über einen Link und über den Missbrauch gültiger Cloud- und lokaler Konten machten jeweils 8 % der Vektoren für den Erstzugriff aus. Datendiebstahl, Datenlecks, Erpressung und Ausspähung galten mit jeweils 25 % als die stärksten Auswirkungen. Auf den asiatisch-pazifischen Raum entfielen 67 %, auf Nordamerika 27 % und auf Lateinamerika 6 %.

5,8 %

der von X-Force bearbeiteten Vorfälle betrafen den Gesundheitssektor.

Nr. 7 | Gesundheitswesen

Das Gesundheitswesen ist auf den siebten Platz der Top-10-Branchen gesunken und ist gegenüber dem sechsten Platz im Jahr 2021 weiter zurückgefallen. In den letzten drei Jahren lag der Anteil der Fälle im Gesundheitswesen, auf die X-Force reagiert hat, bei etwa 5–6 %. In 27 % der Fälle handelte es sich um Angriffe über Backdoors, in 18 % um Web Shells. Jeweils 9 % entfielen auf Adware, BEC, Cryptominer, Loader, Tools zum Ausspähen und Scannen sowie Fernzugriffstools. Mit 50 % entfielen die meisten beobachteten Auswirkungen auf die Ausspähung, während Datendiebstahl und Mining digitaler Währungen in jeweils 25 % der Fälle beobachtet wurden.

Auf europäische Ziele wurden 58 % der Vorfälle nachgewiesen, der Rest (42 %) auf nordamerikanische Ziele.

4,8 %

der von X-Force bearbeiteten Vorfälle betrafen den Verwaltungssektor.

Nr. 8 | Öffentliche Verwaltung

Behördliche Einrichtungen stellten mit 25 % der X-Force IR-Fälle ein weiteres Hauptziel von Backdoors dar. Dieser Prozentsatz entspricht dem von DDoS-Attacken, die ebenfalls ein Viertel der Fälle ausmachten. Die großen Mengen an sensiblen Informationen in den Netzen des öffentlichen Sektors sind ein häufiges Ziel von Cyberspionagekampagnen. Diese Informationen können umfangreiche Datenbanken mit personenbezogenen Daten und anderen Informationen umfassen, die von staatlich geförderten Gruppen genutzt oder von Cyberkriminellen gewinnbringend verkauft werden könnten. Maldocs wurden in 17 % der Fälle identifiziert, während Cryptominer, Tools zum Ausspähen von Anmeldedaten, Ransomware und Web Shells den Rest der Fälle (83 %) ausmachten.

X-Force konnte die Fälle in diesem Sektor zu gleichen Teilen Cyberkriminellen, Bedrohungen von innen, die zur Datenzerstörung führten, Hacktivisten und staatlich geförderten Bedrohungsgruppen zu Spionagezwecken zuordnen.

Die Ausnutzung von Anwendungen mit Internet-Schnittstelle und Spear-Phishing-Anhänge waren mit jeweils 40 % die wichtigsten Infektionsvektoren, während der Missbrauch von gültigen Standardkonten 20 % ausmachte. Mit 50 % der Fälle waren staatliche Stellen im asiatisch-pazifischen Raum am häufigsten betroffen, gefolgt von Europa mit 30 % und Nordamerika mit 20 %.

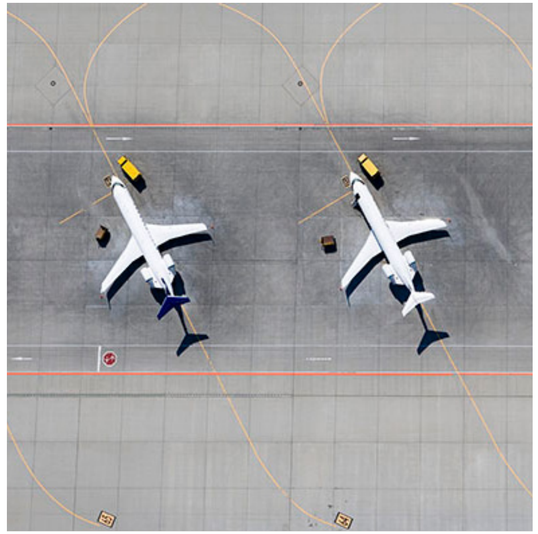
3,9 %

der von X-Force bearbeiteten Vorfälle betrafen den Transportsektor.

Nr. 9 | Transport

Das Transportwesen ist vom siebten Platz 2021 auf den neunten Platz von 2020 gesunken. Der Anteil der Branche an den Vorfällen, auf die X-Force reagiert hat, ist jedoch in etwa gleich geblieben. Phishing war der häufigste ursprüngliche Zugriffsvektor in 51 % der Fälle – gleichmäßig verteilt auf Links, Anhänge und Spear-Phishing-as-a-Service. Der Missbrauch gültiger lokaler Konten machte 33 % der ursprünglichen Zugriffsvektoren aus, während gültige Cloudkonten in 17 % der Fälle als Eingangspunkt dienten. Die wichtigsten Angriffsmethoden bestanden aus Serverzugriffen und dem Einsatz von Fernzugriffstools mit jeweils 25 %, gefolgt von Spamkampagnen, Ransomware, Backdoors und Defacement mit jeweils 13 % der Fälle.

Datendiebstahl trat in 50 % der Fälle am häufigsten auf, Erpressung und Auswirkungen auf den Markenruf in jeweils 25 %. Am stärksten betroffen waren europäische Transportunternehmen mit 62 % der Fälle, gefolgt vom asiatisch-pazifischen Raum mit gut 37 %.



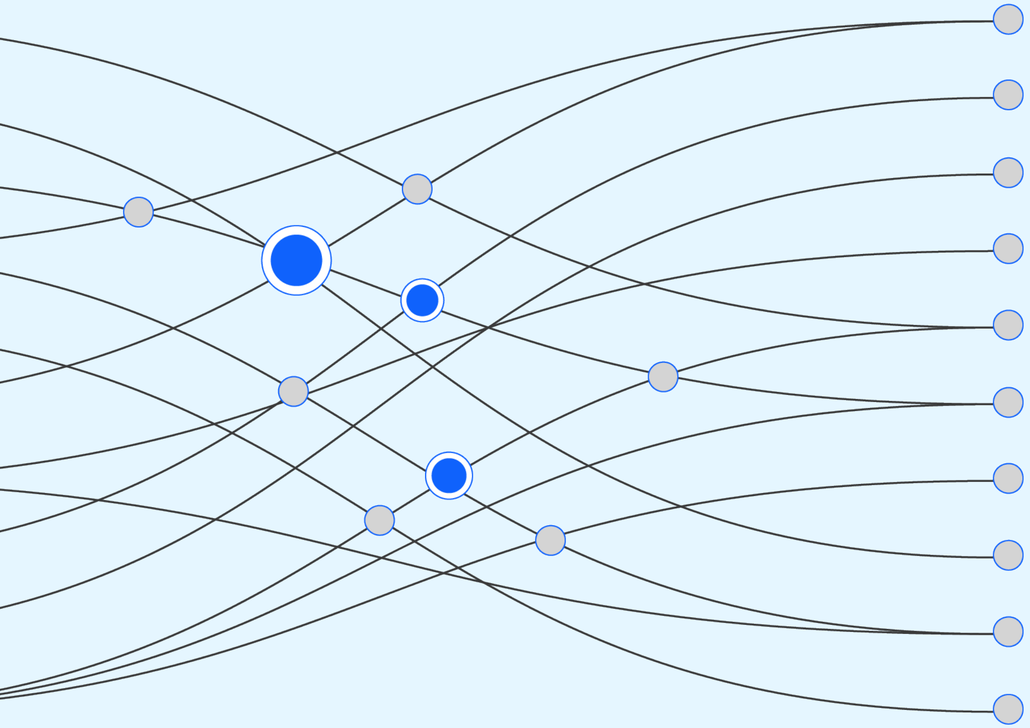
0,5 %

der von X-Force bearbeiteten Vorfälle betrafen den Medien- und Telekommunikationssektor.

Nr. 10 | Medien und Telekommunikation

Den Bereich Medien und Telekommunikation betraf nur einen Bruchteil der Vorfälle, auf die X-Force reagierte, und damit belegte er zum zweiten Mal in Folge den letzten Platz. Als Infektionsvektoren wurden der Missbrauch externer Services per Fernzugriff wie VPNs und anderer Zugriffsmechanismen sowie gültige Domänenkonten beobachtet. Diese Vektoren führten zu Ransomware-Attacken. In diesen Fällen wurden unter anderem Ransomware und Tools zur Datenexfiltration eingesetzt. Dies wiederum zog Datendiebstahl, Datenlecks, Datenvernichtung und Erpressung nach sich.

Empfehlungen



Die folgenden Empfehlungen sind Maßnahmen, die Sie ergreifen sollten, um Ihr Unternehmen vor böswilligen Bedrohungen, einschließlich der in diesem Bericht beschriebenen, zu schützen.

Verwalten Sie Ihre Assets: „Was haben wir? Was möchten wir schützen? Welche Daten sind für unser Geschäft besonders wichtig?“ Das sind die ersten Fragen, die jedes Sicherheitsteam beantworten sollte, um eine erfolgreiche Abwehrstrategie aufzubauen. Die vorrangige Erkennung von Assets in Ihrer Umgebung, die Kenntnis über die Anfälligkeit für Phishing-Attacken und die Reduzierung dieser Angriffsflächen tragen ebenfalls zu einer ganzheitlichen Sicherheitsstrategie bei. Schließlich müssen Unternehmen ihre Asset-Management-Programme auch auf Quellcodes, Anmeldedaten und andere Daten ausdehnen, die sich bereits im Internet oder im Dark Web befinden könnten.

Kennen Sie Ihren Gegner: Während viele Unternehmen die Bedrohungslandschaft aus einem breiten Blickwinkel betrachten, empfiehlt X-Force, sich auf die spezifischen Bedrohungsakteure zu fokussieren, die sich am ehesten auf Ihre Branche, Ihr Unternehmen und Ihre Region als Angriffsziel konzentrieren. Dazu gehört, dass wir verstehen, wie die Bedrohungsakteure vorgehen, wie geschickt sie sind und welche Taktiken, Techniken und Verfahren sie am ehesten anwenden.

Verwalten Sie die Transparenz: Nachdem die Unternehmen mehr über die wahrscheinlichsten Angreifer erfahren haben, müssen sie sicherstellen, dass eine angemessene Transparenz bezüglich der Datenquellen gewährleistet ist, die auf die Anwesenheit eines Angreifers hinweisen. Um Angreifer zu stoppen, bevor sie Störungen verursachen können, ist es von entscheidender Bedeutung, Transparenz an den wichtigsten Punkten im Unternehmen zu schaffen und sicherzustellen, dass Alerts generiert werden und rechtzeitig auf diese reagiert wird.

Hinterfragen Sie Annahmen: Unternehmen müssen davon ausgehen, dass sie bereits kompromittiert wurden. Auf diese Weise können Teams die folgenden Punkte immer wieder überprüfen:

- Wie können Angreifer in ihre Systeme eindringen?
- Wie gut sind sie in der Lage, neue Taktiken, Techniken und Verfahren zu erkennen und darauf zu reagieren?
- Wie schwierig ist es für einen Angreifer, Ihre wichtigsten Daten und Systeme zu kompromittieren?

Die erfolgreichsten Sicherheitsteams führen regelmäßig offensive Tests durch, einschließlich Threat Hunting, Penetrationstests und zielbasiertes Red Teaming, um opportunistische Angriffswege in ihren Umgebungen zu identifizieren oder zu prüfen.

Reagieren Sie auf Grundlage von Informationen: Setzen Sie Bedrohungsdaten überall ein. Durch eine effektive Nutzung von Bedrohungsdaten ist es möglich, gängige Angriffswege zu analysieren, wichtige Möglichkeiten zur Abschwächung gängiger Angriffe zu identifizieren und sehr zuverlässige Erkennungskompetenzen zu entwickeln. Die Anwendung von Bedrohungsdaten sollte mit einer Kenntnis über die Gegner und ihre Arbeitsweise einhergehen.

Seien Sie vorbereitet: Angriffe sind unvermeidlich, aber Ausfälle müssen nicht sein. Unternehmen sollten auf ihre Umgebung zugeschnittene IR-Pläne entwickeln. Diese Pläne sollten an Unternehmensveränderungen angepasst und regelmäßig geübt sowie entsprechend geändert werden, wobei der Schwerpunkt auf der Verbesserung der Reaktions-, Behebungs- und Wiederherstellungszeiten liegen sollte.

Mit einem seriösen IR-Anbieter im Rücken kann die Zeit, die benötigt wird, um qualifizierte Sicherheitsexperten zur Abwehr eines Angriffs zu finden, verkürzt werden. Darüber hinaus ist die Einbeziehung Ihres IR-Anbieters in die Entwicklung und Erprobung von Reaktionsplänen von entscheidender Bedeutung und trägt zu einer effektiveren und effizienteren Reaktion bei. Die besten IR-Pläne sehen eine organisationsübergreifende Reaktion vor, beziehen Stakeholder außerhalb der IT ein und testen die Kommunikationswege zwischen technischen Teams und dem Management. Und schließlich kann die Erprobung Ihres Plans im Rahmen einer Cyber-Range-Übung unter hohem Druck Ihre Fähigkeit zur Reaktion auf einen Angriff erheblich verbessern.

Mehr Sicherheit mithilfe dieser Maßnahmen:

- [ ] Assets verwalten
- [ ] Gegner kennen
- [ ] Transparenz verwalten
- [ ] Annahmen hinterfragen
- [ ] Auf Informationen reagieren
- [ ] Vorbereitet sein

Über uns

IBM Security X-Force

IBM Security X-Force ist ein auf Bedrohungen spezialisiertes Team von Hackern, Respondern, Forschern und Analysten. Das X-Force-Portfolio umfasst offensive und defensive Produkte und Dienstleistungen, die auf einer 360-Grad-Sicht der Bedrohungen basieren.

Im Zeitalter unerbittlicher Cyberattacken, einer vernetzten Welt und zunehmender gesetzlicher Auflagen benötigen Unternehmen einen gezielten Sicherheitsansatz. X-Force glaubt, dass die Bedrohung im Mittelpunkt stehen sollte. Durch Penetrationstests, Schwachstellenmanagement und Simulationen von Angreifern schlüpft das X-Force Red Team von Hackern in die Rolle von Bedrohungsakteuren, um Sicherheitslücken zu finden, die Ihre wichtigsten Vermögenswerte gefährden. Das X-Force IR-Team weiß, wo sich Bedrohungen verstecken und wie sie gestoppt werden können, indem es auf Vorfälle vorbereitet ist, sie erkennt und darauf reagiert sowie Krisenmanagement betreibt. X-Force-Forscher entwickeln offensive Techniken zur Erkennung und Abwehr von Bedrohungen, während Analysten mit X-Force Bedrohungsdaten sammeln und in verwertbare Informationen zur Risikominderung umwandeln.

X-Force weiß genau, wie Bedrohungsakteure denken, strategisch vorgehen und zuschlagen, und kann Ihnen dabei helfen, Vorfälle komplett zu verhindern oder zu erkennen, auf sie zu reagieren und Ihre Systeme nach einem Angriff wiederherzustellen und sich auf Ihre geschäftlichen Prioritäten zu konzentrieren.

Wenn Ihr Unternehmen Unterstützung bei der Verbesserung seines Sicherheitsniveaus benötigt, vereinbaren Sie einen Termin für ein persönliches Gespräch mit einem IBM Security X-Force-Experten.

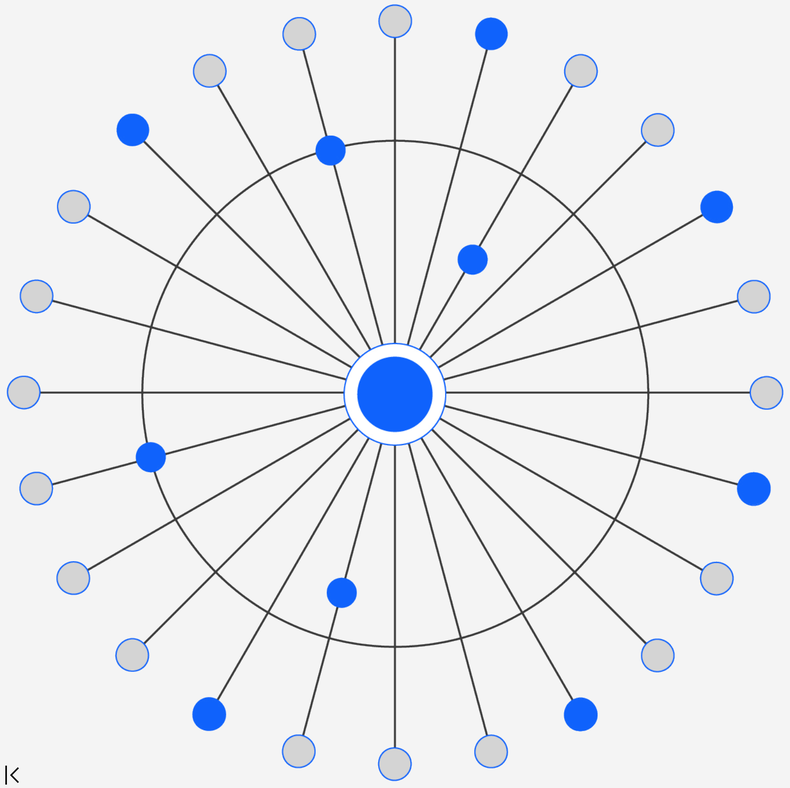
Beratungsgespräch vereinbaren →

IBM Security

IBM Security passt sich Ihrer wachsenden Präsenz an und arbeitet mit Ihnen zusammen, damit Sie auf dem richtigen Weg bleiben. Unsere dynamischen KI- und Automatisierungsfunktionen sorgen dafür, dass Sie immer einen Schritt voraus sind – schneller und genauer. Sie können sicher sein, dass Sie heute und morgen die richtigen Entscheidungen treffen, wenn Sie sich auf die Erkenntnisse unseres zuverlässigen Teams aus branchenführenden Experten verlassen. Von der Bedrohungsprognose bis hin zum Datenschutz, von der herstellerübergreifenden bis hin zur globalen Zusammenarbeit – ganz gleich, in welche Richtung sich Ihr Unternehmen entwickelt: IBM Security unterstützt Sie beim Erreichen ehrgeiziger Geschäftsziele, während Sie sich auf die Entdeckung ausschlaggebender neuer Technologien und Abwehr unerwarteter Bedrohungen konzentrieren.

Mehr erfahren →

Mitwirkende



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

Anhang

Liste der Auswirkungen

Auswirkungen	Auswirkungen
Botnet	Mining digitaler Währungen
Markenruf	Spionage
Ausspähen von Anmeldedaten	Erpressung
Datenvernichtung	Finanzieller Verlust
Datenleck	Produktionsausfälle (OT)
Datendiebstahl	Ausspähung

1. „A timeline of the biggest ransomware attacks“ CNET, 15. November 2021
2. „International action against DD4BC cybercriminal group“, Europol, 12. Januar 2016
3. „DD4BC, Armada Collective, and the Rise of Cyber Extortion“, Recorded Future, 7. Dezember 2015
4. „A Brief History of Ransomware“, Varonis, 10. November 2015
5. „Inside Chimera Ransomware – the first ‘doxingware’ in wild“, MalwardBytes Labs, 8. Dezember 2015
6. „Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware“, Crowdstrike, 14. November 2018
7. „Operators of SamSam Continue to Receive Significant Ransom Payments“, Crowdstrike, 11. April 2018
8. „Triple Extortion Ransomware: The DDoS Flavour“, PacketLabs, 12. Mai 2022
9. „They Told Their Therapists Everything. Hackers Leaked It All“, Wired, 4. Mai 2021
10. „BazarCall to Conti Ransomware via Trickbot and Cobalt Strike“, The DFIR Report, 1. August 2021
11. „Diavol Ransomware“, The DFIR Report, 13. Dezember 2021
12. „Quantum Ransomware“, The DFIR Report, 25. April 2022
13. „Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks“, Kroll, 6. Juni 2022
14. „This isn’t Optimus Prime’s Bumblebee but it’s Still Transforming“, Proofpoint, 28. April 2022,
15. „Understanding REvil: REvil Threat Actors May Have Returned (Updated)“, Unit 42, 3. Juni 2022
16. „AdvIntel’s State of Emotet aka `SpmTools´ Displays Over Million Compromised Machines Through 2022“, AdvIntel, 13. September 2022
17. „Back in Black: Unlocking a LockBit 3.0 Ransomware Attack“, NCC Group, 19. August 2022
18. „Back in Black: Unlocking a LockBit 3.0 Ransomware Attack“, NCC Group, 19. August 2022

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den Vereinigten Staaten von Amerika
Februar 2023